Security & Safety Solutions

Geoffrey V5.1.4

Geoffrey

www.geoffreyaccess.com

User Manual

Table of Contents

Chapter:1 Getting Started 1

Introduction 1

Documentation Conventions 1

Acronyms 1

Key Features 2

System Components 3

Geoffrey Software Default User ID and Password 3

Customer Support 3

Hours of Support 3

Accessing the Application 3

Logging Out of the System 4

Chapter:2 Defining Cardholders 5

Introduction 5

Accessing the Application 5

Overview 5

Add New Cardholders 6

New Cardholder Wizard 6

Credential Definition 10

Add a new Cardholder (Method 2) 22

Duplicate Cardholder Information 22

Adding E-mail Addresses 22

Deleting E-mail Addresses 23

Massive Access Control Modification for Cardholders 23

Delete Cardholders 24

Delete a Single Cardholder record 24

Multiple Cardholder Deletions 24

Export Cardholder Portraits 24

Printing Reports 25

View 25

Image 25

Signature 25

Credential Layout **25**
Cardholder Search Wizard **26**
Find a Cardholder 26
Use of Wildcards 27
Chapter:3 Alarm Monitor 30
Introduction **30**
Alarm Information 30
Starting the Alarm Monitor **30**
Active Alarms **31**
Acknowledged and Not Secured **31**
Acknowledging Alarms **31**
Pre-defined Alarm Comments 32
Receiving Video of Alarms **33**
Viewing and Editing Cardholder Information **34**
Executing Override Tasks **35**
Viewing Previous Alarms **35**
Print Alarm Screen **35**
Minimize Alarm Monitor **35**
Alarm Maintenance **35**
Chapter:4 Previous Alarms 36
Introduction **36**
Accessing the Application **36**
Overview **36**
Running a Report **36**
View Alarm Comments **37**
Options **37**
Tool Bar **37**
Alarm Types **38**
Card Alarms 38
Contact Alarms 38
Relay Alarms 38
Communications Alarms 38
Controller Alarms 39
Operator Alarms 39
System Alarms 39

Guest Alarms 39
Tour System Alarms 40
Chapter:5 Alarm Graphics-Client. 41
Overview 41
Alarm Notification 41
Alarm Acknowledgement 41
Pre-defined Alarm Comments 43
View Cardholder Image 44
Default State of an Icon 45
Search for Icons and Maps 45
Use of Wildcard 45
Advanced Find 45
Chapter:6 Transaction Monitor. 47
Introduction 47
Accessing the Application 47
Overview 47
Working with the Transaction Monitor 48
Defining a Monitor 48
Options 50
Editing Transaction Monitors 50
Connecting to Panels via Dial-up 51
Pausing Transactions 51
Viewing Previous Transactions 51
Accessing Other Applications From Transaction Monitor . . 51
Chapter:7 Previous Transactions 52
Introduction 52
Accessing the Application 52
Overview 52
Running a Transaction Report 52
Printing the Screen 53
Tool Bar Items 53
Transaction Type Definitions 53
Access Granted Transactions 53
Archive History 53
Access Denied Transactions 54

Reader Communications 54
Contact Transactions 54
Slave Controller Communication 54
Reader Controller Transactions 54
Operator Transactions 54
CIM to RC Communications 54
CIM and SP Status Messages 54
Download/Update Status Messages 55
Device Control 55
Guest Pass Transaction 55
Security Tour System Transactions 55
Relay Transactions 55
Chapter:8 Portrait Monitor 56
Introduction 56
Starting the Portrait Monitor 56
Overview 57
Working with the Portrait Monitor 57
Launching the Portrait Monitor 57
Detail View 57
Access Denied Transactions 57
Pausing Transactions 58
Manual Overrides within Portrait Monitor 58
Chapter:9 Audit Trail Report 59
Introduction 59
Accessing the Application 59
Overview 59
Generating a Report 60
Report Dates Available 60
Begin Report 60
End Report 60
Run Report 61
Refresh Report 61
Understanding a Report 61
Column Name Definition 61
Rearranging and sorting Column Titles 62
Chapter:10 Report Launcher. 63

Introduction **63**
Accessing the Application **63**
Overview **63**
Report Tree View 63
Report Groups 64
Base Reports 64
Derived Reports 64
Derived Sub Report (User Created) 64
Launching a Report **64**
Quick Launch Feature 64
Printing and Exporting Reports **64**
Printing 64
Exporting 65
Creating a New Sub Report **65**
Editing a Sub-report 66
Deleting a Sub-report 66
Viewing Report Selections **66**
Chapter:11 Manual Overrides. 67
Introduction **67**
Accessing the Application **67**
Overivew 67
Executing Manual Overrides **68**
Chapter:12 Security Tour System-Client 69
Introduction **69**
Accessing the Application **69**
Overview **69**
Starting a Tour **70**
Description of Fields 70
View Cardholder Image 71
Stop, Pause, Resume Tours 71
Removing Tours 71
Index 72

Chapter 2: Defining Cardholders

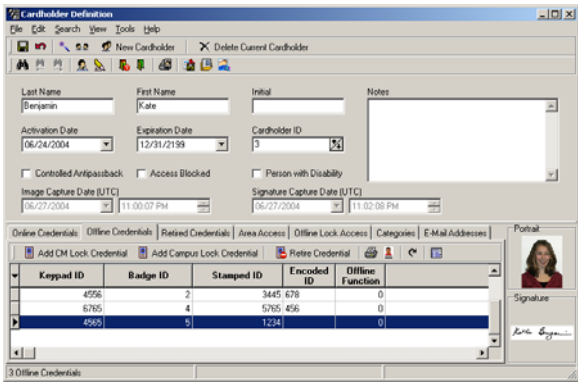
Introduction

The user friendly interface of the Geoffrey Cardholder Definition program allows the user to store the cardholder information easily. The New Cardholder Wizard prompts the user for all necessary cardholder data and provides step by step instruction for adding a new cardholder record. With the help of wizards, all data regarding active and retired badges, area access, cardholder Categories and e-mail addresses are entered and retrieved effortlessly. The user can capture, edit and store cardholder portraits and signatures. The Portrait Enhancement Utility takes the cropped image, enhances it and then displays a selection of 15 photographs. Images can be exported out of the module and sent to any file on your network. There are also options to duplicate cardholder information and print reports. The Advanced Find method helps the user to achieve accurate search results using either simple or complex search options.

Accessing the Application

1. Open the Geoffrey Launcher by double clicking the Launcher icon on your desktop.
2. The login window, opens. Enter your user id and password.
3. In the System Launcher window, double click on **Cardholder Definition** icon.

Overview



The main screen displays the cardholder factory set and user defined fields. The position of the fields are arranged, modified and saved using the UDF Editor module. The lower section of the program displays individual cardholder information regarding badge status, area access, cardholder category and e-mail addresses. Green, yellow and red color indicators are incorporated into the area access time zone and expiration fields. A green indicator shows valid access, a yellow indicator means the access will expire shortly; and red indicates that access has expired.

The system offers multiple options to add a new cardholders into the system. You can use the menu options, tool bars or main screen to accomplish the same task.

The **Cardholder Wizard** is a step by step feature that prompts you for all necessary cardholder data including badge, area sets, area access, category information, image and signature capture. A second option for inputting cardholders is the **New Cardholder** option. This allows you to input the information directly on the main screen. The **Duplicate Cardholder** option is a quick and simple way to enter multiple cardholders who have the same area access and belong to the cardholder category. The program copies these fields from the previous record to a new cardholder record. It will also replicate user- defined fields that are marked for duplication in the UDF Editor module. The user can then enter the new cardholder's name, badge and image information.

Removing multiple cardholder records simultaneously is easily accomplished through the **Delete Cardholders** feature. All these features are described in detail later in this document.

Note: *We recommend you to explore the tool bars icons, menu bar drop down options, hot keys and tabs to be familiar with all the available options within the program.*

Add New Cardholders

There are two ways to enter new cardholder information. They are using the **Cardholder Wizard** and the ***Add New Cardholder* Options**. The Cardholder Wizard will lead you step by step through its screens for cardholder information. The Add Cardholder option allows you to enter information directly on the main screen. However additional steps for image and signature capture are necessary.

New Cardholder Wizard

The **Cardholder Wizard** screens prompts you to add cardholder information, user defined fields, to define badges, add area sets and additional areas for access privileges, cardholder categories and image and signature capture.

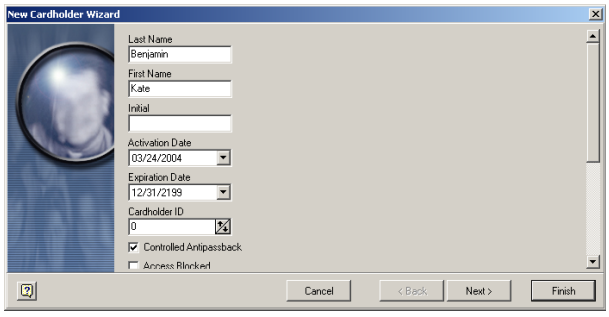
1 Select **File>Cardholder Wizard** option or click the wand icon on the tool bar.

2 The New Cardholder wizard shows all the available fields (the fields that you see on the main screen) including the user defined fields.

I. Last Name is a required field on the first screen. If a User Defined field has been defined in the UDF Editor as "Required" then UDF fields must also be entered as well.

II. User Defined Fields are additional cardholder fields; examples of UDFs are Nick Name, Social Security Number or Phone Extension. Please refer to the UDF Editor chapter for more information. You may type in any of these fields to modify the information. In addition, the date fields offer a drop down calendar. Use the down arrow to scroll for additional fields on the page.

The portrait capture date and signature capture dates are disabled as these dates are entered automatically while adding portrait and signature.



III If you want to block the cardholder's Area Access privileges check the box near the option **Access Blocked**.

IV To enable anti-pass back feature check the box near the **Controlled Anti-pass back** option. If this field is unchecked the card is considered as a master card and it will override the anti-pass back, global anti-pass back rules of the card readers. The card can be used anywhere, any number of times.

Anti-Pass Back

Anti-pass back is a function that prevents cardholders from passing their card to another person for illegal entry. The same card cannot be used at an entry or exit reader twice in a row. In other words, once a card is presented at an entry reader, it must then be presented at an exit reader. If a card is presented twice in a row at the same type of reader, no access will be granted. The Transaction Monitor will display an anti-pass back violation transaction. It is commonly used at car park barriers and turnstiles.

V. If the cardholder is a disabled person, select the option **Person with Disability**. The system identifies valid card reads from persons with disabilities in order to allow access through specific doors with longer GO times (time door strike shall remain energized). The Transaction Monitor displays transactions that differentiate a normal card swipe with a card swipe from a person with a disability. If the field Person With Disability is selected, when the cardholder swipes his/her card the following transactions are displayed instead of the normal “Valid Access” type transactions.

- Valid Access – Person with Disability
- Valid Entry – Person with Disability
- Valid Exit – Person with Disability

VI. Click **Next** to continue to Badge Definition.

Assigning Areas, Area Sets

1 Next, select the Area Sets that you want to assign to the cardholder.

I. Click **Add Area Sets**.

II. Choose the Area Sets from the **Select Area Sets** window. You can use the Search feature to locate Area Sets easily. Click **OK**.

III. Click **Next** on the New Cardholder Wizard.

IV. If you want to assign any other Areas additionally click **Add Areas**. Select the Areas and click **OK**.

V. Click **Next** on the New Cardholder Wizard.

2 **File>Area Access> Add Area Access** option activates the Area Access wizard. There are four different options available on this window.

- **Remove Area Sets -** Removes the Area Set from the cardholder’s record.
- **Set the selected records so that they use the stored template values -** This uses the template values for Area Access permissions that have been defined in the System Manager module.
- **Set the selected records so that they do not use the stored template values -** Allows the user to change time zone, expiration values, area state and door types associated with the Area Access permissions for the specific cardholder.
- **Edit access permissions on the selected Area set -** Allows user to change the Area Set’s access permission for the specific cardholder, provided you have chosen not to use the stored template values.

Your selections will be highlighted in blue color. After clicking **OK**, the wizard will return to the Area Set window.

3 To Delete Area Access, select an Area from the **Area Access** tab and choose delete.

Note: *The Area Access tab in the cardholder main window displays only Areas; it will not display the Area Sets assigned to that cardholder. This means that individual Areas that are members of an Area Set are listed in the cardholder's Area Access tab. An Area will only display one time in the Area Access tab regardless of the fact that it may be in multiple Area Sets that have been assigned to a card. The three buttons are Add Areas, Remove Areas and Edit Areas.*

Note: *Use the Add Area window when a cardholder needs access to a specific area and that Area is not associated with any Area Sets that you've assigned to the cardholder. You may want to skip this screen until you can review the Area Access tab.*

4 Select **Next** to skip this step.

5 In the Area search screen, type the area name in the criteria field or use **Find Now** to display all areas that have been defined.

6 Highlight the Area and choose **OK**. To add multiple Areas, hold the control key down while you make your selections.

7 Click **OK** to display the Areas that have been selected.

Area Access

The Area Access Permission window prompts you for Time zone and Access Expiration. To select a different Time zone, use the browse button. To change the date, use the drop down arrow to access the calendar. The up and down arrows will modify the time field. If the

Click the Advanced button to display all Area States and Door Types.

Note: *If the Area Set(s) you selected is using an Area Access template, the template values will be automatically assigned to the cardholder. The template is defined and assigned during the Area Set definition section in the System Manager.*

1 To assign a time zone and the access expiration time, on the **Area Access Permissions** window, choose the Area Access Time zone. Select access expiration date and time. Click the down arrow near the date field to display the calendar. Adjust the time using the up and down arrows.

2 If you want to block the access, select the check box near the **Access Blocked** field.

3 Click **OK**.

Modify Area Access

1 Select the cardholder record you want to modify Choose the **Area Access** tab located on the lower section of the main screen.

2 Click **Edit the Area Access Permissions** button from the tool bar.

3 On the **Area Access Permissions** window you can edit the time zone and the access expiration date.

Extend Area Access Time

1 Using the **Search** (binoculars) icon on the main screen, choose the cardholder record you want to modify.

2 Click the **Area Access** tab on the lower section of the main window.

3 Select the Area Set. Click **Extend Access to the Selected Areas**.

4 On the **Extend Access Privileges** window, you can adjust the time using the up and down arrows and/or extend the access privilege for a certain number of hours (maximum 8 hours).

Select a Category

1 Now, add this cardholder to any cardholder category that is already defined in the system. You can assign a cardholder to any number of cardholder categories.

I. Click **Add Categories**. Select a category from the list and click **OK**. Add any number of categories you want. Click **Remove Categories** to delete any selected categories.

II. Select **File>Categories>Add to Category** allows the user to add a cardholder record to a cardholder category list.

III. Select **File>Categories>Select a Category** to delete a cardholder from a category.

Portrait Capture

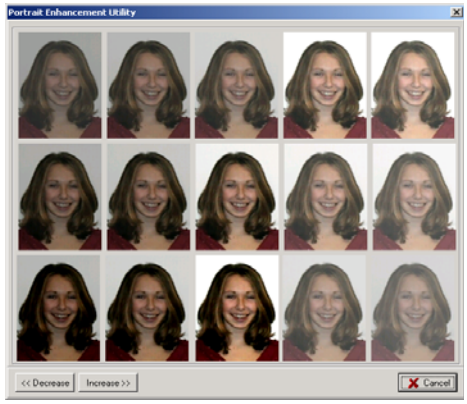
Next step is capture the portrait of the cardholder. Select **Capture** to display the **Cardholder Image** window. Under the **Source** field, your choices are **From File**, **From TWAIN Device** or **From FlashbusMV**. Select **Capture** on the Cardholder Image screen; the photograph is displayed. Tool bar icons offer **Crop Image** or **Show Crop Rubber band** options. The rubber band is used to display a red dotted line. Drag the rubber band to the crop position of your choice then select the Crop Image icon. **Save**, **Cancel**, **Edit** and **Refresh** are not available at this point because the image is stored in memory. Look under the Tools menu for image and cropping choices.

I. **Capture Image -** Click this button to capture the image using the default chosen in the System Manager Settings module. The choices are File, Twain Device or Flash Bus.

II. **Crop Image -** Opens the Portrait Enhancement Utility. Before selecting this option, verify that your Crop Rubber band is placed on the image where you want to crop the photograph.

III. **Cropping Rectangle -** Displays the Crop Rubber band on the image. Drag and resize the rectangle into the position that you want the image to be cropped.

IV. **Portrait Image Enhancer** - This feature is enabled in the System Manager Settings module under the Geoffrey Image Settings tab. When a portrait is cropped, the user is presented with a selection of 15 pictures. Using the Decrease and Increase buttons on the bottom, left of the screen will modify the pictures to make them lighter or darker. Click on the picture of your choice. The window closes and you are returned to the New Cardholder wizard Cardholder Image screen. If you are satisfied with the image select the **Save** icon.



V. Save your changes and close the **Cardholder Image** window. The cardholder portrait is displayed on the New Cardholder Wizard.

Signature Capture

1 Next, you can capture the signature of the cardholder. Click **Capture**. The Source choices are File, TWAIN Device or Geoffrey. If you select the option Geoffrey, you need to have a signature pad connected to the COM Port of your PC. If you select the option From File, the Signature folder is displayed by default. Select the file and click **Open**. The signature is displayed on the Cardholder signature screen. Refer to the previous section in this manual for the tool bar options. Save your changes and close the window. click **Next** on the New Cardholder Wizard.

Credential Definition

Adding credentials is the final step in the cardholder insert wizard. Cardholders may be assigned more than one active credential including one blank badge (a badge with out an encoded ID or a stamped ID). Geoffrey system supports both active online credentials and offline credentials (offline credentials are used for the offline locks). The offline device does not communicate directly with the host controller. The manual programming of the device shall occur at the reader location.

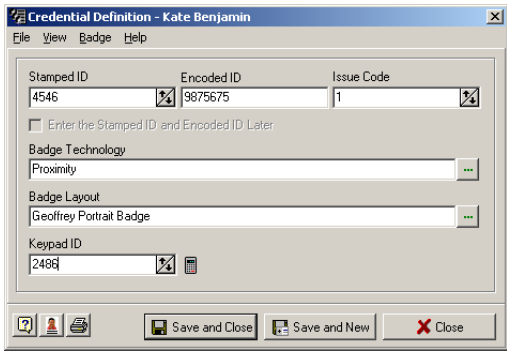
Active Online Credentials

Active online credentials are used for the readers that communicate directly with the host controller. Follow these steps to define the online credentials.

Add Credentials

1 Select the tab **Active Online Credentials**. Select **Add Credential** to open the **Credential Definition** screen.

Note: *One badge per cardholder can be added without entering a stamped ID or an encoded ID. Check the option "Enter the Stamped ID and the Encoded ID Later". If the current cardholder already has a blank badge (a badge without a stamped ID or encoded ID) the* ***Badge Definition*** *dialogue will not allow the user to create another blank badge.*



I. Badge Technology and Badge Layout are required fields. Badge Layout displays the list of layouts that have been created in the Badge Creation module.

Note: *Privileges to select, view or print badges will be based on the operator's security group permissions set in the System Security Module. When permission to a badge layout equals none, selecting, viewing or printing that layout will be unavailable.*

II. Stamped Number is the pre-printed number located on the back of the cardholder's badge.

III. Issue Code counts the number of badges issued to an individual cardholder. The original credential will have Issue Code 1.

IV. Once you fill in the required fields, select **Save and Close**. Click **Save and New** to add another badge. The information will display in the grid window. Once you are done with adding badges click **Finish**.

Active Credential Options

There are eight options available under the Active Credentials sub-menu. Selecting from the Active Badge sub-menu links to badge fields and opens the Active Badge tab.

1 Select **File>Active Credentials**. The following are the menu options.

I. **Add Credential -** open the Badge Definition window.

II. **Retire Credential -** Highlight a badge then select this option to remove it from the Active Online Credential tab and write it to the Retired Credential tab.

III. **Reset Anti pass back State -** Returns the cardholder's anti pass back state to neutral.

IV. **Select Credential Layout -** Opens the Credential Layout Description window that allows the user to select a different layout.

V **Print Credential -** Allows user to send the highlighted credential to either the default credential printer or a print queue.

VI **Calculate Keypad Pin -** Uses the Encoded ID of the highlighted badge to calculate a PIN number. Standard or Geoffrey PIN Encryption is defined in the **System Settings** module.

VII. **Edit Badge -** Click on this option to edit badge technology and badge layout. Stamped ID, Encoded ID and Issue Codes are displayed as Read Only fields.

Generating Credentials Automatically

The Cardholder Definition program allows the user to create badges automatically. This feature saves your time because if badge automation feature is enabled in the System Settings, whenever you click **Add Credential** or captures a cardholder image the system generates badges automatically. The user has to create a user-defined field and link it (using UDF LINK program) with the badge technology and the badge layout they will be using in the automatically created badges.

This badge automation functionality works in two different modes.

- **Credential Insert Partial Automation Mode**

In partial automation mode, an online credential is created when the user clicks the Add Credential button.

- **Credential Insert Full Automation Mode**

In full automation mode, an online credential is created only when the cardholder image is taken.

Credential Insert Partial Automation Mode

The following criteria must be met to insert an online credential automatically.

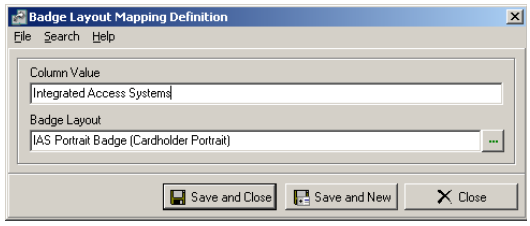
- There should not be an existing blank credential (a blank credential is one without encoded id and stamped id) for the cardholder.
- Valid UDF Cross References must be created for the badge technology and badge layout.

Note: *If there is no valid UDF Cross Reference, a dialogue pops up asking you to select the badge layout and badge technology.*

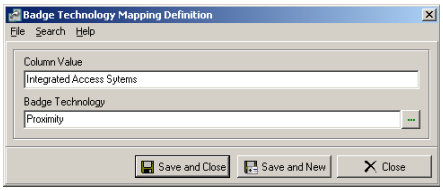
- The user must have at least read only permissions to the cardholder record.
- The user must have as least read/write permissions for badging.
- The option **Credential Insert Partial Automation Mode** must be selected in the System Settings.
- The option **Enter Encoded ID and the Stamped ID Later** must be selected in the System Settings

Follow these steps to insert a blank credential:

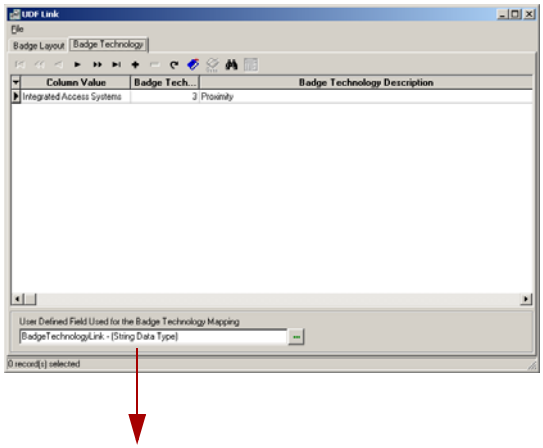
1. Design badge layout and annotations necessary for creating badges.
2. Create a user-defined string field that can be duplicated using the UDF Editor. For example create a string field called “Badge Technology Link”.
3. Using the **UDF Cross Reference** program, link the field you created with a badge layout and a badge technology. In order to do this first, the Badge Layout Mapping must first be defined. Assign a logical column value. For this example, Geoffrey Industries is typed in the Column Value field. Whenever this value is entered in the relative field in Cardholder Definition, the program will automatically create a badge using the badge layout you have specified here.



4 Next define the badge technology mapping.



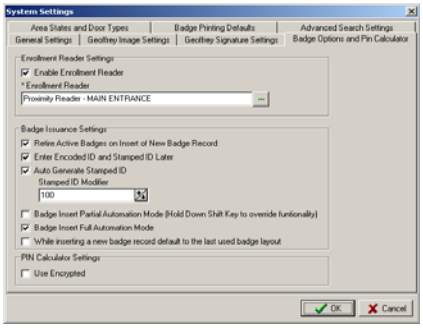
5 Select the user-defined field that you want to use for badge technology mapping. (You can use the same user defined field that you used for badge layout mapping.)



Select the User Defined Field here

6 In the System Settings, select the following options.

- Enter Encoded ID and Stamped ID Later
- Badge Insert Partial Automation Mode


System Settings
Area Sates and Door Types
Badge Printing Defaults
Advanced Search Settings
General Settings
Geoffrey Image Settings
Geoffrey Signature Settings
Badge Options and Pin Calculator
Enrollment Reader Settings
Enable Enrollment Reader
* Enrollment Reader
Proximity Reader - MAIN ENTRANCE
Badge Issuance Settings
Retire Active Badges on Insert of New Badge Record
Enter Encoded ID and Stamped ID Later
Auto Generate Stamped ID
Stamped ID Modifier
100
Badge Insert Partial Automation Mode (Hold Down Shift Key to override funtionality)
Badge Insert Full Automation Mode
While inserting a new badge record default to the last used badge layout
PIN Calculator Settings
Use Encrypted
OK
Cancel

7 Click **OK**. If Cardholder Definition program is already open, close the program and open it again.

8 Add a new cardholder. In the user defined field that was linked to badge automation, type the same column value that was entered in the Badge Layout Mapping Definition (of UDF Cross Reference). For example, enter “Geoffrey Industries”. This is the value that was used as our example while mapping the field with badge layout and technology. So whenever you enter the field value of the user-defined field, and click Add Badge button the system will automatically generate a blank badge.

Note: *You have to make sure that the UDF you have created is linked properly using the UDF Cross Reference program. Otherwise a dialogue pops up asking you to select the badge layout and badge technology.*

9 Click **Add Credential**. An online credential is automatically inserted.

Credential Insert Full Automation Mode

When Badge Insert Full Automation Mode is on, badges are generated automatically after the cardholder’s photograph is taken for the first time.

The following criteria must be met to insert a blank badge in the Full Automation Mode.

- There must not already be a blank badge (a blank badge is one without Encoded ID and Stamped ID) for the cardholder.
- Valid UDF Links must be predefined for Badge Technology and Badge Layout.
- The user must have at least read only permissions on the cardholder.
- The user must have as least read/write permissions for badging.
- The option Enter Encoded ID and the Stamped ID later must be turned on in the System Settings
- The option **Credential Insert Full Automation Mode** must be turned on in the System Settings.
- The **Image Date** field must be blank.

Now follow steps 1 to 5 in the Badge Insert Partial Automation Section.

Once you have created the user-defined field and linked it with a particular badge technology and badge layout, you can start adding cardholders.

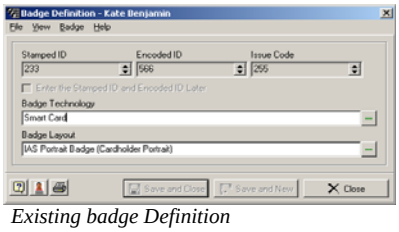
Fill in the required fields. While filling in the user defined field that you used for linking with the badge technology and badge layout, make sure that you are using the same field value that you used for linking.

Note: *The field value in Cardholder Definition must be the same as the column value that was entered in the UDF Cross Reference module.*

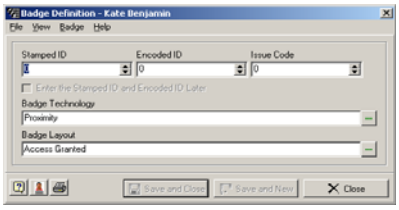
If the system is set to **Badge Insert Full Automation** mode, a blank badge is created when the user captures the photograph of the cardholder for the first time.

Editing Credential Information

You can edit an existing credential by double clicking on the badge fields on the main window of Cardholder Definition program. You can change badge technology and badge layout. If the badge is a blank one you will be able to edit all the fields.



Existing badge Definition



Blank badge defintion

Offline Credentials

The Geoffrey System supports offline readers which does not communicate with the host controller directly. So it is necessary to do manual programming at the reader location. The user can create necessary downloadable files and upload to a pocket PC. The data is transferred to a PDA by connecting to the serial communication port of the PC. The programming of doors is accomplished by connecting a **CIP** (Computer Interface PAK cable) from the laptop/palmtop to the iButton ports of the lock.

Geoffrey supports two types of offline readers, CM Locks and Campus Locks.

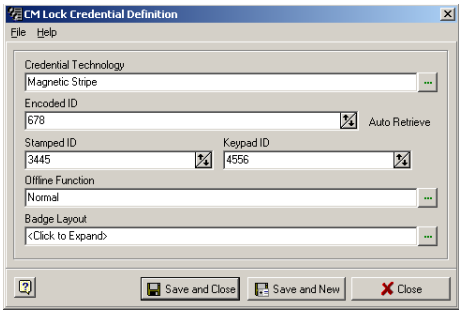
Adding CM Lock Credentials

Follow these steps to define CM Lock Credentials for cardholders.

1 Select the **Offline Credential** tab. To define a new offline credential, select **Add Credential**.

Note: *This tab will be visible only if the user has at least read only rights to the System Manager security item Badges and has at least read only permissions to one of the cardholder fields in the grid. If these conditions are not met, the tab and the corresponding main menu options (File>Offline Credentials) will not be available.*

2 The **Offline Credential Definition** window opens.



Fill in the following fields:

I. **Credential Technology** - Select the type of credential technology.

Note: *Credential Technology field cannot be changed when the dialog is in edit mode. The credential must be retired and a new one should be created to change this field. This field must be entered before saving the record.*

II. **Encoded ID, PIN, or iButton** - This field changes depending on what the credential technology you have selected in the previous step. It can be one of three different types:

a. **Encoded ID** - This field is for card types (Magstripes, proximity etc); the maximum length of the encoded ID is 16 digits.

Click the **Auto Retrieve** option to automatically retrieve the Encoded ID, PIN or iButton ID by attaching an offline lock to the computer through a serial port. When the user touches the button or swipes a card at the reader, the system generates the ID automatically.

b. **PIN** - This field is for PIN Only credential types. It must be numeric value between X and 8 digits. X = a setting in System Settings under Offline Credential Settings called ***Minimum PIN Length***. The minimum digits that the system allows is 3. The smaller the minimum length, the smaller the amount of PIN number the system can have.

Ten digit versus five digit PIN and other PIN rules

CM Lock hardware supported by Geoffrey access control system does not work with full ten digit PIN, but converts PINs to a five digit scheme representing the buttons on the lock's keypad. Although all ten digits can be used, the resulting PIN is converted into the five digit scheme and, then tested against all other five digit PINs in the system. Only when no duplication with another five digit PIN is detected, the new PIN will be accepted. The translation is as follows:

Digits in PIN	Translated Value	Button label on lock's keypad
1,2	1	1.2
3,4	2	3.4
5,6	3	5,6
7,8	4	7,8
9,0	5	9.0

This means that the PINs "13579" and "24680" are considered to be identical. Furthermore, PINs that are a subset of an already existing PIN are not allowed. For example, when PIN "13579" already exists in the system a PIN “1357” is not accepted. Also, it is highly recommended to use the **Auto Retrieve** option to generate the PIN, and not to use birth dates or other restricted or easy to guess sources. The system uses the Minimum PIN Length specified in the System Settings while generating the PINs.

c.**iButton** - This option is used for iButton credential types. The ID must be 16 digits in length and can only have hexadecimal characters (0.9, a.f).

Note: *This feature is only used for iButton credential types. The Credential Technology must be selected before using this feature.*

COM Settings

The COM Port must be configured in System Settings under the Offline Credential Settings tab called Offline Enrollment Reader COM Port. If the COM Port is not configured correctly, the feature will time out after a set amount of seconds.

The time-out period can be set under **System Settings> Offline Credential Settings >Offline Enrollment Reader Time-out**. The default is 5 seconds, but you can change this value to have enough time to swipe the credential. The time-out

starts as soon as the button is clicked.

If this feature is used only for proximity cards, the setting in **System Settings>Offline Credential Settings>Proximity Card Format** must be selected. If this field is set incorrectly, an error will occur and the system cannot retrieve the Encoded ID from the badge.

Note: *This is a required field.*

III. **Stamped ID** - This field is enabled only for card credential types; it is the number actually printed on the badge.

Generating Stamped Id Or Encoded Id Automatically

The encoded ID and Stamped ID fields can be generated automatically by enabling a setting in **System Settings >Offline Credential Settings>Stamped ID Modifier**. Enter a value in this fields which functions as the modifier of the stamped ID or encoded ID. It works by taking the Encoded ID and subtracting the Stamped ID Modifier to get the Stamped ID and vice versa.

If the above option is enabled, when the Encoded ID is entered by the user, the Stamped ID will automatically be generated using the above calculation. If the Stamped ID is entered by the user, the Encoded ID will be automatically generated.

Note: *This field must be between 0 and 2,147,483,647. If the Stamped ID modifier makes this field greater than 2,147,483,647, the field will just be 0 then.*

IV. **Keypad ID** -This field is only enabled for Card and iButton types. The **Generate Keypad ID** button can be used to automatically generate the Keypad ID.

Note: *Keypad ID also can be generated. It follows the same input rules as the PIN Encoded ID above.*

Note: *Keypad ID value zero means there is no keypad ID.*

Note: *A cardholder can have two credentials with same Encoded IDs as long as the Keypad IDs are different.*

V. **Offline Function** - Click on the expand button to select a function the offline credential will perform when the cardholder presents the credential at the door.

Note: *This is a required field.*

These are the offline functions available.

a. Normal - Normal opens a door for a specified time. The time span is defined by the Relock Delay set in the Offline Lock Definition.

b. Toggle - Toggle opens a door and leaves it open until it is closed again by a toggle credential. It toggles a door between locked and unlocked.

c. Freeze - Freeze disables the keypad/credential reader. Only credentials set to “Pass Through” can open the door. Use a credential with “Freeze” function to return the door to an operational state. “Freeze” does not lock a door, for example when the door was toggled open.

d. One Time Use - One Time Use opens the door only once with the Normal function. After the door relocked the credential does not work anymore on this door. It can still work on other doors, until after it was used on these doors once.

e. Pass Through - Pass Through is a credential function that allows Users to pass through doors that are in secured lockout mode. It does not matter if this mode was set by a door Holiday, or by a Freeze credential used when the door was secured. A Pass Through credential will open the door for the specified relock time.

f. Dogged - Dogged has only a special function on electronic dogging bars. On these exit bars it keeps the push pad pushed in and the door unlocked. Dogged works as Normal function on all other devices.

g. Supervised - Supervised credentials follow the "two person rule" Two supervised credentials must be used within five seconds to open the door. The door stays open until the Relock Delay ends.

h. Prohibit Access (with Alarm) - Prohibit Access (with Alarm) is a credential function that will not allow the credential to open a door, but it will register when the User of this credential tries to do so. It always generates an Audit Event, and additionally sounds the Alarm when the door is equipped with a horn.

i. CT Aux - This credential function operates only the Auxiliary relay of CT Controllers, but not the Main relay. The time span the relay is activated is specified by the Relock Delay.

j. CT Main and Aux - This credential function operates both the Auxiliary relay and main relay of Controllers. The time span the relays are activated is specified by the relock delay.

VI. **Badge Layout** - Select a layout for the badge. This is the layout the badge uses when previewed or printed.

Note: *This field is enabled only for card technologies. This is not a required field.*

Note: *This dialog follows cardholder field security permissions. If the user does not have at least read only rights to a field, it will not be visible. The user must have read/write permissions to all required fields in order to save a record.*

Automatically Create CM Lock Credential

The Geoffrey system allows the users to automatically create a corresponding offline credential when a new online credential is created.

Follow these instructions to generate an offline credential.

1 Open System Settings program. Enable **Offline Credential Settings>Automatically create an offline credential when an online credential is created** checkbox.

Note: *Only users with administrator rights to System Settings will be able to modify this field because it is a global setting throughout the system.*

---

2 Create a new online credential with an Encoded ID. Keypad ID is optional. This feature will not work with credentials created with no Encoded ID. Save the record.

3 The application then verifies that the same cardholder does not already have an offline credential with the same Encoded ID and Keypad ID. If the user already has a offline badge that meets these criteria, then the process stops there. The system does not generate any error message.

If the cardholder does not already have an offline credential with same encoded ID and Keypad ID and, an error occurs during the process, the user will be notified of this error with a message dialog.

The offline credentials grid will be refreshed and the new credential will be visible.

Editing CM Lock Credentials

If you want to make any changes to the offline credentials you have created, double click on the record to open it. Make the necessary modifications and select **Save and Close**.

Exporting Data

1 To export the offline credential data to a directory in your hard drive, select the record, and right click on it.

2 Select the option **Export Data** or **Export and Open Data**.

3 Choose the directory where you want to export the data.

4 Choose the correct format you want to save the data. Available formats: .xml, .html, .txt, .csv (comma separated value).

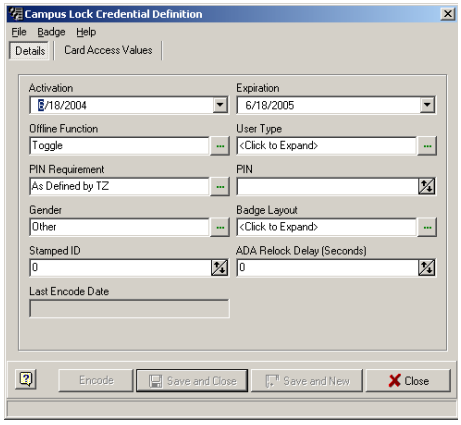
5 Give a file name. Click **Save**.

Campus Lock Credential Definition

Unlike CM Locks Campus Locks are assigned by generating Credential data which is encoded on the magstripe card. Access Rights assignments are therefore tied to the Magstripe card and require the mag card to be present for encoding.

Follow these steps to assign a Campus Lock Credential to a cardholder.

1 Select the Offline Credential tab. Now choose, Add Campus Lock Credential button. In the Campus Lock Credential Definition window, the **Details** tab displays the following fields.



I. **Activation** - Select a date that the credential will start providing access to the selected locks.

II. **Expiration** –Click the drop down arrow to select the expiration date for the credential. This is the date the credential will expire. This must be at least one day greater than the activation date. The time the expiration will expire can be changed in the Campus Lock Definition dialog in System Manager.

III. **Offline Function** – Offline function specifies the behavior of the Campus Lock Credential. Generally, the selection in Function is the only place to specify Campus Credential behavior, but there is one exception. Campus Locks can be configured to allow Campus Credential with "Normal" function to toggle the lock open or close when swiping the card twice. The options available in offline function are described in page #15 & 16. Click on the expand button to see the list with all functions. Select the desired function by clicking on the function name in the list. The list closes and the new selection appears in the text field of function

IV. **User Type** – Select a user type this credential is part of. All the enabled user types will be shown in the list. Select the desired user type by clicking on the label in the list. The list closes and the new selection appears in the text field of User Type.

V. **PIN Requirement** - PIN Requirement specifies whether a PIN is also required while presenting a card to get access. The mandatory use of a PIN can be enforced for all times, can be required during a Timezone that is assigned to a User Type, or can be never used. Accordingly, the available options in PIN Requirement are "As Defined by TimeZone", "Always", and "Never". Click on to see the list with the options and select the desired option by clicking on the specific entry. The list closes and the new selection appears in the text field of PIN Requirement.

Note: *When setting up Timezones that require PIN use, make sure that this Timezone includes all times during which a user type is supposed to have access to that lock. When users are supposed to be allowed to access a campus lock without mandatory PIN entry during some times and with mandatory PIN entry during other times multiple Timezones have to be set up in* Timezone Definitions.

***Example*:** All Users with user type "Administration" are allowed to enter a Door between 8 AM and 6 PM without entering a PIN. During the time spans 6 AM to 8 AM and 6 PM to 8 PM a PIN entry is mandatory. Between 8 PM and 6 AM any user with user type "Administration" is not allowed to access the lock. This setup requires three TimeZones to be set up.

VI. **PIN** - Enter a value that the credential will use after it is swiped at a campus lock. This is required if the PIN Requirement is set to Always or As Defined by TZ. If the PIN Requirement is set to Never, then this does not need to be entered.

VII. **Gender** – Campus locks can be set to allow access rights for male or female users only, or to conduct no check on gender. Click on to see the list with the options "Male", "Female", and "All" and "Other". Setting Gender to "Male" allows access rights to locks that are set to "Male" or "All", setting Gender to "Female" allows access rights to locks that are set to "Female" or "All", and "Other" allows Access Rights to locks that are set to "Other" or do not check gender access. Choose the desired setting by clicking on the list entry. After the selection is completed the list closes and the new selection appears in the text field of Gender.

a. All means this credential can get in all locks no matter what gender access is checked.

b. Male means this credential can only get into locks that have male access only or that do not check gender access.

c. Female means this credential can only get into locks that have female access only or that do not check gender access.

d. Other means this credential can only get into locks that have Other access only or that do not check gender access.

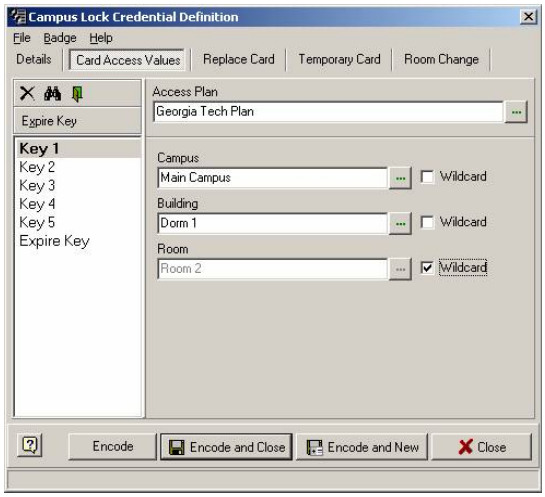
VIII. **Badge Layout** – Select a badge layout of the credential. Click on the expand button to see all the defined badge lay outs. Select a layout and the list closes. The selected layout will be displayed in the Badge Layout field.

IX. **Stamped ID** – Enter the ID number printed on the badge. This allows the user to distinguish between different credential just by looking at the credential. This must be between zero (0) and 2,147,483,646.

X. **ADA Relock Delay** – An individual ADA Relock Delay can be assigned to each Campus Lock Credential. The ADA Relock Delay of a credential always overrides the standard Relock Delay time configured for a lock. It further enables the ADA Relock Delay function of a Campus Lock. When both Campus Lock Credential and Campus Lock have an ADA Relock Delay specified, the longer delay time of both will apply, even when it is shorter than the standard Relock Delay of the lock. Enter the delay time in seconds into the text field of ADA Relock Delay (Sec.) or use to increase or decrease the delay time. The default entry is "0" and the maximum amount is 255 seconds.

XI. **Last Encode Date** – This displays the last time the credential was encoded. This is a read only field.

2 Next step is selecting the access plan that this credential will have access. Select the **Card Access Values** tab. This tab is used to setup the card access value keys for the credential. Access to a particular building, floor or room is given by associating its value to a key. A credential is allowed to have a maximum of five normal keys and one key that will expire on a set date. Multiple keys may be needed for the credential to have access to all the doors. The left part of the tab shows the 5 keys and the 'expire key'. Captions that are bold mean that a key is currently defined for that key. When a key is selected, the right part of the tab shows the access plan and the values that the key is currently using. The new access right assignment will not take effect unless the credential is encoded.



I. To assign a key, first select a key and select an access plan that is already defined in the system. To assign a key, you need to have at least one access plan defined.

II. When a plan is selected, the system displays all the properties and values associated with that particular plan. The controls that you see on this screen depend heavily upon the access plan properties and values defined using the Access Plan Definition program. This means that the names shown may be different for each access plan. The property values can be selected by clicking on the expand button next to each property. When you click on the button, the corresponding property values are displayed. The user then must select a value for each property or select the Wild card checkbox which makes it a wildcard. All properties must completely be entered or the key will be invalid and the credential cannot be saved. The delete button above the keys will clear the selected key.

III. You can set a key to expire on a specific date by setting it as an Expire Key. This option is useful when it is necessary to grant a user temporary access rights to two rooms at the same time, for example when moving from one room to another. Instead of assigning access rights to the additional room and then keeping track manually in order to remove the access right after a few days a credential can be encoded to allow access rights for two rooms up until a specified date. At this date access rights to the first room expire and only access rights to the new room are in place. Once a key is set as an Expire Key, a Key Expiration Date should be selected. This date cannot be set more than a year from the current date. The minimum date is one day after the current day. This key will no longer be valid after this date. The Expire Key cannot be manually altered. It must be a duplicate of an existing key. Only the 'Key Expiration Date' can be changed. When a normal key is selected as an expire key, the properties for the access plan will be loaded.

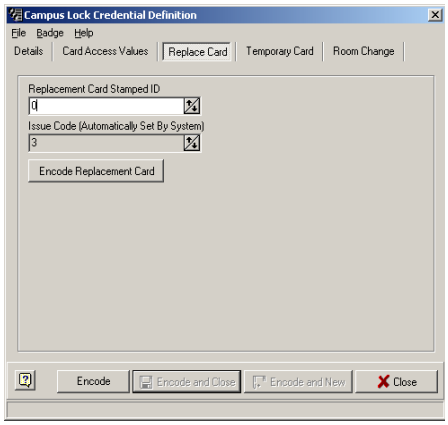
3 At least one key must be defined to save the credential. Each key can have a separate access plan if wanted.

Encoding a Credential

Any change to a Campus lock credential is only submitted to the database after the credential tied to the currently opened credential record is encoded with updated information. Clicking Encode will first initialize the Card Encoder connected to the PC. A message text appears in red font above the button bar of Campus Lock Credential Definition dialogue. Once the initialization is completed the card encoder is set to write mode and is ready to encode the Campus lock credential. Insert a card into the card encoder when the read/write light of the encoder turns on. A message indicates that the card is successfully encoded.

Replacing a Card

Geoffrey system provides functionality to limit the damage resulting from a lost Campus lock credential. This tab will only display after the credential has been encoded once and the credential is being edited. It allows the operator to replace a lost credential. The **Encode Replacement Card** button will increment the issue code by one and then encode the new card. The new issue code will only be saved if the encoding process is successful. The new card must be swiped once to disable the lost one. This issue code cannot be manually changed. This system just uses the next value. The first time a card is encoded, the issue code is zero.



Also the user need to enter the Stamped ID for the replacement card that is printed on the new card. This replaces the old stamped ID that is in the database.

Temporary Card

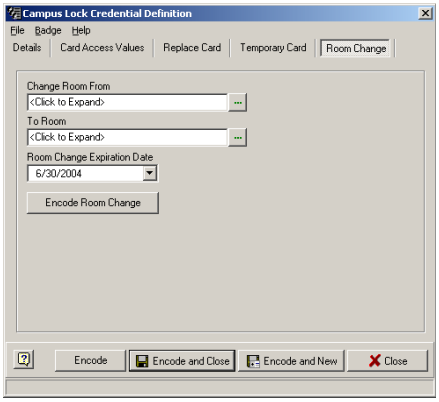
This tab will only display after the credential has been encoded once and the credential is being edited. This allows the operator to issue a temporary card to a cardholder. If the card is completely lost, the replace card option should be used instead. The maximum expiration date can be set using the System Settings application. The default is seven days. This means that the longest this card can last is seven days from the current day. The activation must be the current day or above and must be one day below the expiration date.

·The **Encode Temporary Card** button will encode the temporary card using the dates selected.

Room Change

Note: *You need to encode the credential at least once to have the Room Change tab available.*

The Room Change tab is a simpler interface for the expire key feature. While using the Room Change feature, instead of the user selecting an existing key, and converting it to an Expire Key, the user can select the lock they want to expire on a specific date and then can give access to a new lock. The user need to then select the expiration for the room change.



1 **Change Room From** lists all the Campus locks that are assigned to the currently selected credential. Click of Change Room From to see a list of all Campus locks and select the one to change by clicking on the specific entry in the list. The list closes and the new selection appears in the text area of Change Room From.

2 Click **To Room** to select the room to change to. Assigning a new lock for a Room Change works the same way as assigning an additional lock with the exception that only one lock can be created. The **Change Room To** lookup list only shows locks the user currently does not have access to.

3 The **Room Change Expiration Date** option allows the user to select the expiration for the room change. The minimum date is one day after the current date and the maximum date is one year after the current date. A Room change is typically used to allow a person to move things from one room to the other. In order to prevent this person from keeping access rights to the previous room the Room change expires at a specific date. From that date on access rights to the previous room are dropped and only access rights to the new room are in place. Select the expiration date in Room Change Expiration Date. The default date is always one day after today.

4 Once all the controls have been filled in, the user must use the **Encode Room Change** button for the changes to take affect. This will save the record with the room change and then encode the new card. The user must present the same card that matches the database.

Define Offline Lock Access

Note: *This option applies only to the CM Lock credentials. Campus lock access privileges are defined using the Campus Lock Access Definition dialogue.*

The next step is defining the access privileges for the offline credentials you created. Follow these instructions to define offline lock access for credentials.

1 Select the tab **Offline Lock Access>Add Offline Lock Access** or select **File>Offline Lock Access>Add Offline Lock Access** .

2 Click the + (insert) sign on the upper part of the **Define Offline Access for...** window.

3 Select the credentials that requires access to a specific area. The Insert button opens the search window allowing the user to select any of the current cardholder's offline credentials.

4 Once credentials have been added, the user then must select the credential you want to add access for. The system allows the user to create multiple access records for a selected credential. You cannot add offline lock access to more than one credential. at a time.

Note: *The selected credentials displays in bold characters.*

5 Once the credential has been selected, the user can use the bottom pane to select the locks to add access to. · The insert button in the bottom pane brings up the **Offline Lock Access Definition** dialog. The system allows the user to select multiple locks for one credential.

6 Select the expand button and selected a time zone. This is a required field. You cannot select locks until a timezone is selected. This is because each lock has different time zones attached to them, up to 16, and when searching for locks, the system only displays locks that have the selected time zone attached.

7 Now select the activation and expiration dates by using the down arrow located near the corresponding fields.

8 Select the + (insert) sign to add the locks. As mentioned above, only locks that have the selected time zone will be available for selection. At least 1 lock must be selected before saving. The user can add the same locks to the same credentials as long as the time zone is different.

9 Select the **Save and Close** to save the record.

Note: *An offline lock can only support 1000 access records.*

Click the delete button in the bottom pane to remove the selected locks from the list view for the selected credential.

The edit button in the bottom pane will bring up the **Offline Lock Access Definition** dialog in edit mode with the current access record.

Retire Credentials

The **Retire Credentials button** allows the user to retire active credentials whenever they like. This option is particularly useful if a credential is lost or stolen. In such a situation the operator can issue a new credential to the cardholder and retire his/her old credential. This feature helps the users ensure security.

1 Select **Active Online Credentials** or **Offline Credentials** tab, highlight the credential that you want to retire. Click the **Retire Credential** button on the tool bar. You can also retire a credential by selecting **File>Active Credential/Offline Credential>Retire Credential** option. The credential no longer has any access control privileges. *(The EncodedID from this badge may be reused immediately.*) The credential is automatically removed from the **Active Credentials** tab and can be found under the **Retired Credentials** tab. In the **System Settings** program under Badge Options and Pin Calculator section, select "**Retire Active Badges**" option. If you have checked this option, each time you initiate a new badge for the cardholder, a window pops up to select the active badges to retire.

Note: *Please note that the lock has to be programmed for any change to take place.*

2 Select **Reactivate Credential** option to reactivate a retired credential.

Add a new Cardholder (Method 2)

1. A second way to add a cardholder is to fill in the fields on the main window. If you have specified any user defined field as *Required* in the UDF Editor, then a value must be entered in that UDF field as well.
2. Click **Save** on the tool bar once you have populated the fields in the top section. After the Save button is clicked, the tabs in the lower section of the window become active.
3. Enter information for Badge, Area Access, Category and E-Mail. Capture an image or signature using the tool bar icons or by accessing them from the View menu bar.

Duplicate Cardholder Information

This function is designed to help you to avoid typing repetitive data for new cardholders. It is useful when you must enter multiple cardholder records that will have the same Area Access and category privileges. It will also replicate user- defined fields that are marked for duplication in the **UDF Editor** module. The default data will appear in the tabs after the required fields are entered. Badge, image and signature information is entered individually for each cardholder record.

1. To use the **Duplicate Cardholder** option, first display an existing cardholder record with the same area access and cardholder information or enter a new record with area access and category information that you want to be copied. Now click on the **Duplicate Cardholder** tool bar icon or select it from the File menu.
2. Enter the cardholder information in the top section of the screen and click the **Save** icon. Area Access and Category information appears.
3. Click the **Active Badges** tab and choose **Add Badges** to display the **Badge Definition** window. Here you must enter an Encoded ID, Badge Technology and Badge Layout. The Stamped Number and Issue Code are optional fields.
4. Next you can capture images and signatures. For pictures, choose the **Capture Image icon** on the main screen tool bar or chose Image from the View menu. The Cardholder Image window is now displayed. Choose your Capture Source then select the Capture button on the bottom left corner. Your cropping options become active on the tool bar and in the Tool menu bar option. When you are satisfied with the image click **OK**.
5. To open the Cardholder Signature window, select the Capture Signature icon on the tool bar or choose Signature from the View menu. This feature works exactly like the Capture Image screen.

Adding E-mail Addresses

Cardholder's e-mail addresses can be stored in the system. The user can either insert new E-mail addresses or associate the cardholder information with the existing addresses that are stored in the system using E-mail Address Editor application. This option is also equipped with a search feature that allows you to find records easily.

1. To add a new E-mail address, select the **E-mail Addresses** option from the lower pane of the window and choose the + (plus) icon.
2. On the Insert E-mail Addresses window, type in the E-mail address. You can add as many records you want.
3. Click **OK**. The records are shown in the **Address** section of the main screen.
4. You can also select the existing E-mail addresses and associate with a cardholder information. Select **Associate Existing E-mail**.
5. On the Search window, enter the text in the ***Search Criteria*** field and click **Find Now**. Just clicking the **Find Now** button displays all the records defined in the system. Select the appropriate records and click **OK**.

Deleting E-mail Addresses

1. If you want to remove an e-mail address from a cardholder record, open the cardholder record and select the E-mail Address tab located in the lower section of the window.
2. Select the e-mail address you want to delete and select the delete icon from the tool bar.
3. A confirmation message is displayed. Choose **Yes** to continue.

Note: *If the e-mail address you are trying to delete is attached to a report (used in the Report Scheduler program) you can not delete the record. A warning message is displayed preventing you from deleting the record.Modifying and Deleting Cardholders or Cardholder Information*

Cardholder data can be modified and deleted directly from the main screen and by using menu or tool bars. Locate and display the cardholder by using the Search feature. You may type over information in any fields in the top section of the window then use the tabs and the tab tool bars to change badge, area access and category information.

The grids of tabs cannot be modified. The quickest way to modify a field is to click on the record and use the picture icons. To edit a Date field use the drop down arrow to display the calendar or type the change directly in the field. Highlight the year field and right click your mouse to open the shortcut named “Go to today”. The field displays the current date.

To delete information on a cardholder, highlight the field within one of the tabs and select the appropriate delete icon from the tab tool bar. To delete a cardholder from the database, search and display the cardholder then chose the Delete Cardholder icon.

Massive Access Control Modification for Cardholders

The Cardholder Definition program provides functionality to mass modify Access Control fields of cardholder records (modifying more than one cardholders at a time). The fields you can mass modify are Access Blocked, Activation and Expiration Dates and Controlled Antipassback.

Follow these steps to Mass Modify Access Control fields for more than one cardholders at a time.

1. Select **Tools > Modify Access Control for Cardholders**. The following window is displayed.
2. Select the cardholder records by clicking **Add Cardholders**. You can use the Search and Advance Search features for adding cardholders. Once you have added the required cardholder records you want to modify, click **Next**.
3. In this step you must select the access control fields you want to modify.
   - **Access Blocked:** Check the box to enable this field (This sets it’s value to true.). If you want to block access for the selected cardholders click the box next to the field.
   - **Activation Date:** Enable this field by clicking the check box. You can modify the activation date by entering the date manually or click on the drop down arrow to use the calendar. Make sure that the date you enter is a valid date. (It must be the current date or a future date.)
   - **Expiration Date:** It works the same way as the activation date. Enable the field and select a valid date.
   - **Controlled Antipassback:** Place a check mark in the box next to Controlled Antipassback, if you want to enable this functionality.

4 Click the **Next** button to continue. A summary of the modifications you made is displayed. To change any value, click **Back** to return to the previous step. When you are satisfied with the modifications, click the **Finish** button to complete the process.

Delete Cardholders

Delete a Single Cardholder record

1 Using the Cardholder Search wizard, select the cardholder record that you want to remove from the database.

2 With the record displayed on the main screen, select **Edit>Delete Current Cardholder** or choose the tool bar icon. A confirmation message is displayed. Click **Yes** to delete the cardholder.

Multiple Cardholder Deletions

In the Cardholder Search wizard, choose the records to be removed from the database. This feature is separate from the Delete Cardholder icon that resides on the tool bar.

While deleting multiple cardholders at the same time, any attempt that fails will be added to a list view and when the deletion is complete, a dialog pops up with a list of cardholders who were not deleted and showing the cause of the error.

1 Select **Edit** > **Delete Multiple Cardholders** or select the tool bar icon. The Cardholder Search window will display. Use your control (Ctrl) key to make multiple selections. Click **OK**. A confirmation message is displayed to verify the number of cardholders to be deleted. Click **OK**.

Export Cardholder Portraits

This feature provides an Export Wizard that sends cardholder images to a separate file. These files can reside on the local drive or can sent across the network to and saved on a different computer. This is useful when you want to store image copies on a different server or when a picture needs to be attached to an E-mail message. It is recommended that the Export file reside outside of the Geoffrey software.

1 The Export Wizard permits you to copy portraits to a new file located outside of Geoffrey software. The **Add Cardholder** button links to the Cardholder Search Wizard. Highlight your selections and click **OK**.

2 A list displays when a portrait will not be exported. The wizard displays the cardholders selected for export.

3 The next step is to select the path, file naming convention and file name separator.

I. **Directory for Export:** Type the full path or use the Browse button to select your folder location.

II. **File Naming:** The Export folder will contain the JPG images of your cardholders. Select a good naming convention under the File Name section. When choosing a combination of fields, you can determine the order by using the Field Up and Field Down buttons.

III. **Separator:** This is used in conjunction with file names that use several fields.

Example: When using a period, the file name format in the folder will be Last.First.jpg such as Doe.John.jp

A forward slash, back slash or star symbol is not permitted as a Separator. An error message will display if one of these characters are entered.

Printing Reports

Print Dossier Report: A Dossier is a type of Badge Layout that has been identified as such in the Badge Creation module. A Search window allows the user to select from a list and send the report to be printed.

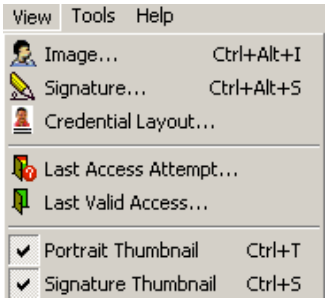
Dossier Reports can be sent to queues just like badges. While printing the reports select the option *"**Send Dossier Reports to Printer Queue**."*

Note: *The system will default to the option set in the System Settings program. In the System Settings if you have set the option as "Send Dossier to Default Printer" the system will automatically defaults to that option.*

If you have set a default dossier queue in the System Settings the system will default to that dossier queue automatically.

Print Portrait Export Report: This report is created and printed when the user selects the date of the file export.

View



Image

This selection opens the Cardholder Image screen. The user can capture a picture or manipulate the image utilizing the tool bar icons, Crop Rubber band, Crop, Edit and Save. Image settings for this window are enabled in the System Manager Settings module.

Image screen options

Crop Rubber band: Selecting this icon activates the red cropping band. Drag the edges of the band to change the area of the picture. (*In the System Settings module, "Allow Crop Rubber band to be Moved or Sized" must be checked to set the value to true.*)

Crop: This option will trim the picture to display only what is inside the red cropping band.

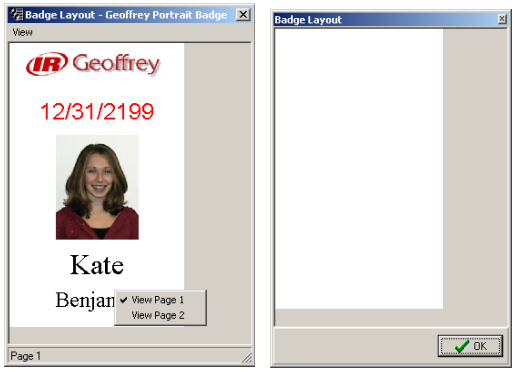
All th eatures are available through the tools menu.

Signature

This feature opens the Signature Image screen. The user can capture a signature or manipulate the image utilizing the crop and edit features. Signature options work like the image screen.

Credential Layout

1. On the Active Online Credential/Offline Credential tab, highlight a credential then click the Credential Layout icon to view the cardholder's badge.
2. You can also view the back of the image. Right click on the badge and click on **View Page 2** from the option.



Last Access Attempt

The **Access Attempt** window provides Transaction, Cardholder and Reader information fields. It displays the last time a cardholder has swiped a card at a reader regardless of whether they were granted or denied access.

Last Valid Access

This window contains the cardholder's most recent **Valid Access** information such as transaction date and time, cardholder and reader information.

This is very useful when you must immediately find a cardholder's last known location.

Portrait Thumbnail

If this option is selected the system shows a thumbnail image of the cardholder in the lower pane of the main window of the application.

Signature Thumbnail

If this option is selected the system shows a thumbnail image of the signature of the cardholder in the lower pane of the main window of the application.

Cardholder Search Wizard

Find a Cardholder

When you click on the binocular icon, the Cardholder Search Wizard is activated. There are three search features. They are Find Cardholder, Find Previous Cardholder and Find Next Cardholder. You can search by Last Name, First Name or User Defined Fields.

To view the entire cardholder database, press the Find Now button without entering a value in any field. ***The default search order is displayed alphabetically***. To search by a user-defined field, place a check mark in the UDF Search field and fill in the values.

Previous in Search: This will display the previous cardholder in the database according to the sort order that was selected in the above option.

Next in Search: This will display the next cardholder listed in the database according to the cardholder sort order.

Show Results on Load: This search feature is intended to be used the first time the module is opened. Checking one of the sub-menu items will load all the data when the search form is opened. An unchecked item will display a blank search form and the user must enter values for the search.

To change the sort order, left click on a column heading. For instance, to sort by Cardholder ID, click on the Cardholder ID title bar. *Your sort order directly affects Previous Cardholder in Search and Next Cardholder in Search*. Size and order of columns can be changed by dragging and dropping to a new location. The bottom left corner of the screen will display the number of cardholders that have been selected

Advanced Find Feature

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The Advanced Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use.

The saved search criterion is displayed only for the operator who defined it.

Cardholders can be searched using cardholder fields (like first name, last name etc.), badge criteria or activation and expiration date.

1 Click on the Advance Find tab located on the top of the Search window.

2 The Advance Find of Cardholders window opens.

3 Click on the Cardholder Fields button to search for cardholders by field name.

4 Define your search criteria.

I. If you want to search for Cardholder ID = 10, you need first select the left parenthesis from the list box.

II Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.

III Select Cardholder ID as the Field Name.

IV Select equal to (=) as the condition.

V Enter the value as 10.

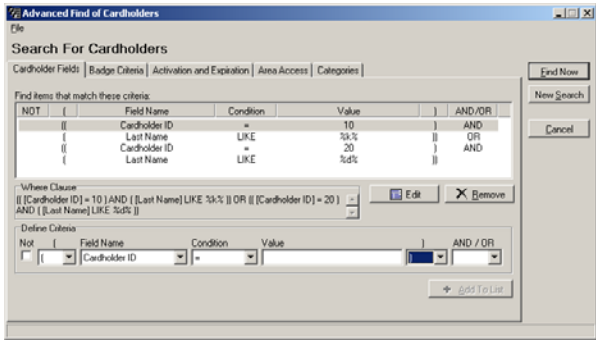
VI Provide the closing parenthesis at the end.

VII When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.

VIII If you would like to specify additional search condition you can select AND/OR from the list box.

E.g. If you want to search Cardholder IDs less than or equal to 10 and last names with the letter “K” and Cardholder IDs greater than or equal to 20 and last names with the letter “D”, define the search criteria as follows.

((Cardholder ID>=10) AND (Last Name Liked%)) OR ((Cardholder ID>=20) AND (Last Name LIKE%d%))



When you run the search you will get the records corresponding to your search criteria. The following window shows the search result.

5 Once you have defined the criteria click **File>Save**.

6 Add a description to your search and click **OK**.

7 The new search will be saved for future use and listed under the Advanced Find button.

You can also search for cardholders using Badge Criteria, Activation and Expiration Date, Area Access and Categories.

Use of Wildcards

The Advanced Search feature provides ways to select certain cardholder records without typing complete information. Geoffrey System allows the use of wildcards (more formally known as *metacharacters*) to stand for one or more characters in a cardholder record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the% (percent sign) as a **wildcard**. Within the search criteria, a user can type the% character before or after their search text as a wildcard.

E.g. Entering *%er* will return all the last names that end with the letters "*er*". By using the wildcard in the beginning, the user is requesting the system to find all parts that ends with "*er*" and could have additional characters in the beginning.

Berner

Creager

Kaiser

Entering%er% will return all the last names that contain the letters *"er"*.

Anderson

Berner

Creager

Kaiser

Roberts

Slathers

Wildcard has a very flexible capability to help users identify specific information based on limited or partial search information. One thing to note; however, this capability can result in very large query results if misused.

Exporting Search Results

Cardholder search results can be exported to your hard drive in the following formats:.xml,.html,.txt,.csv (comma separated value).

To export search results to your hard drive,

1 Run a search and right click on the search results.

2 Click the **Export Results** button.

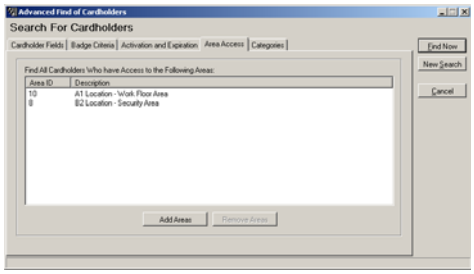
3 Choose the directory to which you want to save the results. Give a file name. Click the drop down menu to choose an available file format.

4 Click **Save** button to complete the action and the search results will be saved in your system.

Note: *Exporting Cardholder Search Results feature is also available in the* ***All Cardholders*** *tab in the System Manager module.*

You can also search for cardholders based on their area access.

5 Select the **Area Access** tab on the **Advance Find** window.

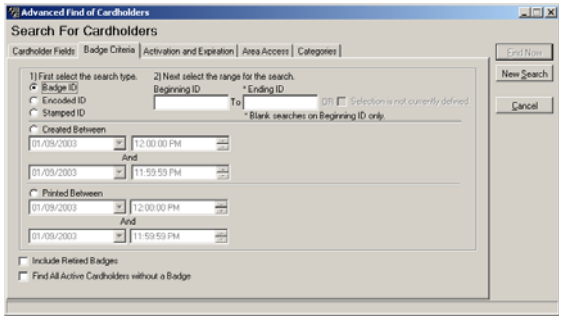


6 Select the Areas to which the cardholders you want to find have access by clicking on the **Add Areas** button. You can run a search to find the areas easily. Select the areas and click **O**.**K**.

7 Click the **Find Now** button in the **Advanced Find for Cardholders** window.

8 The search results are displayed in the **Search** window.

Badge Criteria Tab



Search by Badge ID, Encoded ID, Stamped ID or badge creation dates by clicking in the circle and entering the information.

When a search is run by Badge ID, Encoded ID or Stamped ID, you can select a range between the Beginning ID number and Ending ID number.

For example, if you would like to search for all cardholders that have been issued badges for the last seven days, click in Creation Between and use the calendar drop down to select the dates. Click the Find Now button to initiate the search. You can also search for badges that have neither Encoded ID nor Stamped ID (blank badge). For example, place a check mark next to EncodedID. Next, check the box ***Selection is not currently defined*** *and* run the search. You can see that all the badges that don't have Encoded ID are displayed.

You can also check the option to ***Include Retired Badges*** and ***Find All Active Cardholders with out a Badge***.Categories

Follow the same procedures described above to search for cardholders based on their categories. Instead of Area Access select the **Categories** tab, and add categories.

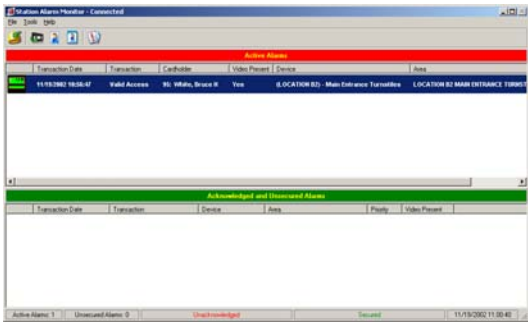
Selecting A Cardholder

Highlight a cardholder and select the **OK** button. The application returns you to the main window and displays the cardholder's information. Once a cardholder is open in the main window, the **Find Previous Cardholder** and **Find Next Cardholder** icons become active. The Previous and Next search are based on the current sort order.

Chapter3:Alarm Monitor

Introduction

The **Alarm Monitor** gives you flexible and programmable monitoring of virtually any alarm condition. It is a program that helps you to view, acknowledge and secure all alarms that you have defined in your system. There are two types of Alarm Monitors. The first is a Workstation Alarm Monitor, which displays alarms that are programmed to appear on predefined workstations. The second is an Operator Alarm Monitor, which displays alarms wherever selected operators are logged into the system. An E-mail Recipient can be defined, as well, to receive messages upon specific alarms. Procedures for defining the Alarm Monitors are covered in the preceding Alarm Definition chapter.



Alarm Information

When an alarm is triggered, the system sounds an alert and displays the Alarm Monitor screen at a designated Workstation or at the location(s) where Alarm Operators are logged on.

The highest priority alarms will be at the top of the screen, indicating they require immediate attention. A User ID and password, comments or other actions may be required in order to acknowledge an alarm, depending on how it was programmed. E-mail recipients can be created and receive instant notification when critical alarms are triggered.

If the alarm has a **Sound File** attached, when the alarm occurs, the system plays the recorded sound file. The sound file can be attached with the alarm, when the alarm is defined in the Alarm Definitions program.

Starting the Alarm Monitor

Note: The Alarm Monitor icon will not appear in the System Launcher.

This module must be added to the **Start up** tab in **System Security** for each workstation that is to receive alarms. To do this, go to **System Security\Startup**, click **Add** and select Alarm Monitor.

Note: *If a Workstation is not attached as part of a routing group, Alarm Monitor cannot be enabled.*

If an alarm operator logs into a computer that is *not* defined as an alarm workstation, or where the **Alarm Monitor** is not placed in the **Start-up** tab, the Alarm Monitor will still open as long as the alarm operator is defined as part of a routing group.

When the alarms appear, only users with the proper rights will be able to acknowledge. Remember to give the proper Alarm Monitor Privileges (at least *Read-Only* rights) to the users that are defined as Alarm Monitors or they will not be able to respond to the alarms.

Active Alarms

This section displays incoming alarms and those are not acknowledged. The color schemes for the alarm display are customized in the Alarm Definition module.

Acknowledged and Not Secured

Certain alarm transaction types relate to the normal physical state of a device. When the normal state changes, an alarm is triggered. While the alarm may be acknowledged, it will display in this section until the device has physically been returned to the normal state. The example below shows a Controller Alarm for a CIM Lost Link to RC. This alarm will remain here until the connection to the controller has been restored. The transactions, or conditions that will secure these types of alarm are Contact Secure, Restored Link to Reader, Restored AC Power to RC, Battery Power Normal at RC, Communications Restored to Slave Controller and CIM Restored Link to RC.

Acknowledging Alarms

When an alarm occurs, the system alerts the operator by popping up the Alarm Monitor on the screen. The alarm remains on the screen until the operator acknowledges it.

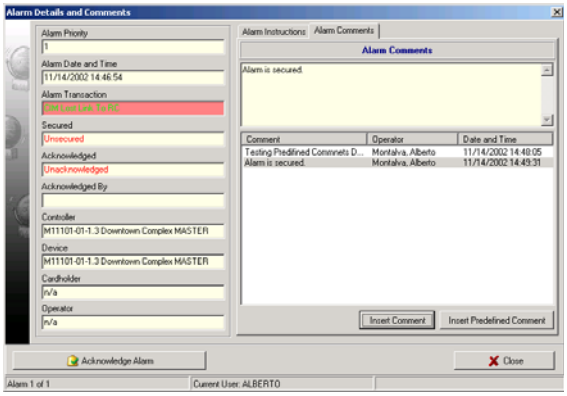
As a part of establishing standards for alarm acknowledgement, the administrator can set parameters that force the operator to enter comments either free-form or by selecting pre-defined comments. The parameters can be set while defining alarms in the Alarm Definition program.

Follow these steps to acknowledge an alarm.

1 Select the alarm that you want to acknowledge from the Alarm Monitor screen. Right click on the alarm and select the option **View Alarm Details** from the menu.

You can also access the Alarm Details window by selecting **View Alarm Details** option from the **File** menu or double clicking on a selected alarm.

2 The **Alarm Details and Comments** window is displayed.



The left hand side of the Alarm Details window displays the following information.

I. **Alarm Priority:** This indicates the level of priority of the alarm.

II. **Alarm Date & Time:** The date and time the alarm has occurred is displayed in this field.

III. **Alarm Transaction:** The transaction that caused the Alarm.

IV. Secured: Whether the device that is attached to the particular alarm is secured or not.

V. Acknowledged: Whether the alarm is acknowledged or not.

VI. Acknowledged by: The name of the Operator who acknowledged the alarm.

VII. Controller: The controller that is connected to the device which generated the alarm.

VIII. Device: The device that generated the alarm. (E.g. In a situation where there is an alarm called "Lost Link to Reader", the Reader is the Device. The name of the Reader will be displayed in this field.)

IX. Cardholder: If the alarm is a cardholder alarm, the name of the cardholder will be displayed here.

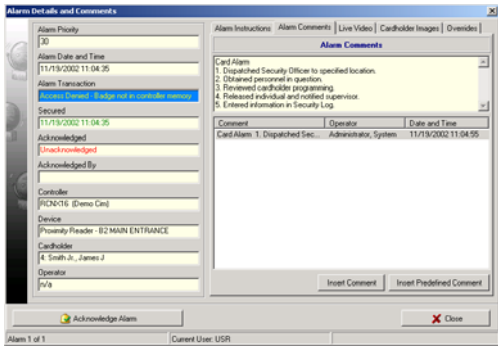
X. Operator: If it is an operator alarm (E.g. illegal login) the name of the Operator will be displayed in this field.

The right hand side of the window contains Instructions to the Operator and the comments that are added by the operator.

3 Click on the **Alarm Instructions** button to see the instructions to the Operator. These instructions are entered in the Alarm Definition program, when an alarm is defined. The administrator can attach a .wav file with each instruction.

4 Depending on how the alarm was defined, you may be required to provide User ID or comments for the highlighted alarm before the system will accept the acknowledgment command. The administrator can "*force login*" and "*force comments*" before letting an operator to acknowledging an alarm. If this is the case, the applicable window will open for you to enter said requirements and acknowledgment will be accepted.

5 While entering comments you have the option to select the predefined comments or enter comments free- form.



The above screen capture shows, an example of comments for an Access Denied transaction.

Pre-defined Alarm Comments

Geoffrey System provides a program for the Administrator to set pre-defined comments for the operator to enter while acknowledging the alarms. Follow these steps to define alarm comments.

1 Open the **Pre-defined Alarm Comments** program from the System Launcher.To add new set of comments, click on the plus sign in the **Pre-defined Comments** window.

2 Enter the comments in the **Pre-defined Comments Definition** window.

3 Click <**Save and Close**> to save the application and return to the main window. Click <**Save and New**> to save the current definition and define a new one. Click <**Close**> to close the Definition window with out saving the defined comments.

While defining alarms, the administrator can attach these comments with the alarm. The operator shall be able access these comments from the **Alarm Details** window while acknowledging the alarms.

Receiving Video of Alarms

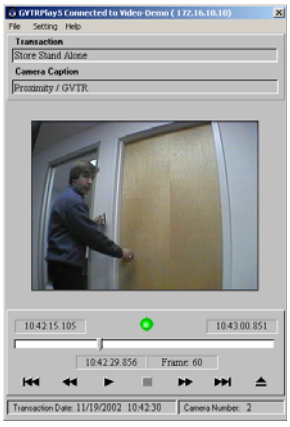
If there is Geoffrey Digital Video Transaction Retrieval System attached to your Geoffrey Access Control System, you can receive video of each transaction that occurs in the system. The Alarm Monitor is capable of displaying live and recorded video. The recorded video is displayed in a separate window so that the user can still view the live video while viewing the recorded video.

1 You can play the video by clicking on the video icon on the main window.

View video of a transactions

2 The video of the transaction from the camera is displayed on your monitor screen. This helps you to get potential information of all the alarms.

You can perform the playback back functionality using various buttons appear on the screen.



Note: *For further information on Geoffrey Video Transaction Retrieval System, refer to GVSD user and installation manual.*

To receive video of transactions in the Alarm Monitor, the user has to define the transactions, device that generates the transaction and the camera that is associated with it etc. in the GVTR module.

The user also has to define transactions as Alarms in the Alarm Definitions program to receive alarms.

You can also receive live video on the Alarm Monitor while viewing the recorded video of a transaction.

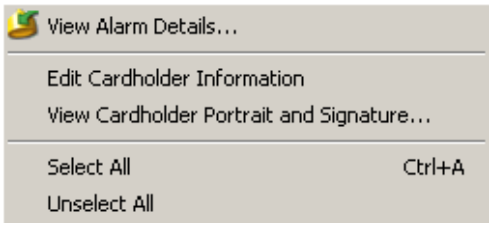
In the **Alarm Details** window click on the button **Live Video**. The video from the camera associated with the transaction will be displayed on the screen.

3 Click on the **View Recorded Video of this Alarm** button to play back the video of the alarm. This video file is opened in a new window so that display of live video is not interrupted.

Viewing and Editing Cardholder Information

Alarm Monitor also allows you view the portrait and signature of the cardholder (provided you are viewing a card alarm) in question to reassure the security further.

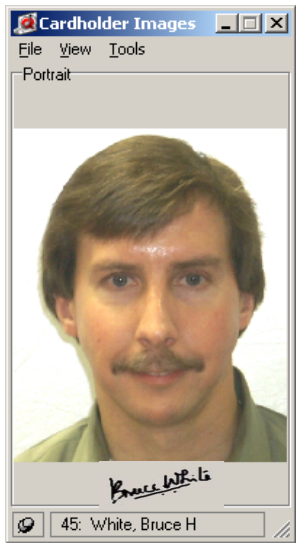
1 Right click on the Alarm and choose **View Cardholder Images** option from the menu.



or click on the tool bar icon shown below.

View the portrait and signature of the selected Alarm

2 The cardholder portrait and signature are displayed.

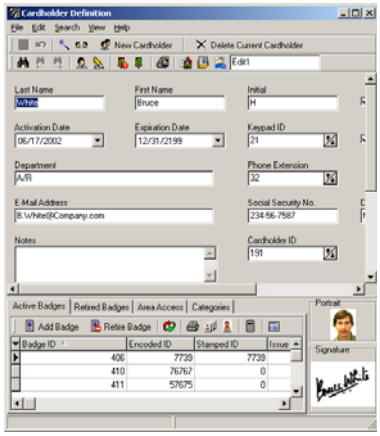


3 The user can choose to view either portrait or signature only or clear both. Click on the **View** menu and select the appropriate option.

4 If you want to snap the Portrait window to the corner of the screen, click on the **Tools>Options**. In the settings window specify the number of pixels at which you want to snap the window to the right or left corners.

5 You can also view or edit the information about the cardholder in question. You can access the Cardholder Definition program from the Alarm Monitor screen itself, and edit the information. This feature helps the Operator to give or deny access to a particular cardholder. To perform this functionality, the Operator must have *Read/Write* privilege to the Cardholder Definition application.

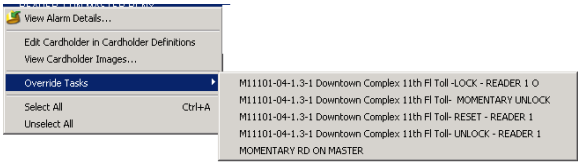
6 Right click on the transaction and select **Edit Cardholder in Cardholder Definitions Program**.



Executing Override Tasks

When an alarm occurs, the operator can execute necessary actions using the Override Tasks that are defined in the system. The system shows all override sets and tasks that have the alarmed device as an associated device for the override tasks or the device that the action affects for an override action.

To execute these Override Tasks, right click on a alarm and select **Override Tasks** from the menu, and click on the override you want to execute.


View Alarm Details...
Edit Cardholder in Cardholder Definitions
View Cardholder Images...
Override Tasks
Select All Ctrl+A
Unselect All
M11101-04-1.3-1 Downtown Complex 11th Fl Toll -LOCK - READER 1 O
M11101-04-1.3-1 Downtown Complex 11th Fl Toll- MOMENTARY UNLOCK
M11101-04-1.3-1 Downtown Complex 11th Fl Toll- RESET - READER 1
M11101-04-1.3-1 Downtown Complex 11th Fl Toll- UNLOCK - READER 1
MOMENTARY RD ON MASTER

Viewing Previous Alarms

If you want to view alarms that occurred previously, click on the *View Previous Alarms* from the **File** menu. It opens the program for running reports on alarm history. Details for this module are found in Chapter 4.

Print Alarm Screen

To print the current display of Alarm Monitor, click on the *Print Alarm Screen* button from the **File** menu.

Minimize Alarm Monitor

Clicking on the *Minimize the Alarm Monitor* option from the **File** menu will minimize the screen to the task bar; if alarms exist that have not been acknowledged, the screen will continue to pop up until they are attended.

The Close command is not available on the Alarm Monitor screen. The module cannot be closed down on an Alarm Workstation without exiting the Launcher and the Access Control System completely. An Alarm Operator must log off to close the Monitor. If you want to snap the alarm monitor window to the right or left corners of the screen, click on the **Tools** menu and click ***Options***. In the **Settings** window specify the number of pixels at which the Alarm Monitor window snaps to the corner of the screen.

Alarm Maintenance

The Alarm Maintenance is a utility used for trouble-shooting purposes. It is used to retrieve, display, select and remove alarms from the SP buffer. Acknowledging alarms, comments and video retrieval will not be available. This window displays active and secured alarms that are currently held in the memory buffer. You can quickly view the alarm details and its transaction details.

1 To delete an alarm, highlight the number and transaction and use **Delete Alarm**.

2 To update the screen click **Refresh View**.

3 Select the check box **Auto Refresh** to update the screen automatically.

4 To close this window, select **Done**.

Chapter4:Previous Alarms

Introduction

The View Previous Alarms module gives an accounting of alarms that have occurred and the comments attached with it. You have the ability to select the type of alarm, the date and time range of activity, running a specific report to the screen and printing it out.

Accessing the Application

1 Open the Geoffrey Launcher by double clicking the Launcher icon on your desktop choose **Start>Programs>Access Control SystemV5>System Launcher**.

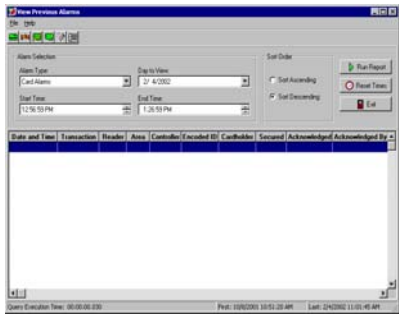
2 The login window, opens. Enter your user id and password.

3 In the System Launcher window, double click on **Previous Alarms** icon.

Note: *You can also open the View Previous Alarms module through the Alarm Monitor.*

Overview

The main screen consists of the menu and tool bars, alarm selection, sort order and report controls, display grid, and the status Bar. Details follow for all screen features.



Running a Report

In order to run a report of alarms that occurred in the system you need to first specify the alarm type, date and start and end time.

1 First select the alarm type. The down arrow will open the Alarm type selection menu. The different alarm types available to choose from are Card, Contact, Relay, Communications, Controller, Operator, System, Guest, and Tour Alarms. You can only choose one alarm type at a time.

- Then select the day to view. The current date is the default. Click on the down arrow to display the calendar and click on the day you wish to view. A red circle appears around today's date and the day chosen will be highlighted.

2 Use the up and down arrow to adjust the start and end time of the alarm reports.

3 Then select the sort order. You can select either Sort Ascending or Sort Descending.

4 Select **Run Report**. This will execute the query and displays the information

5 To reset the start and end time, click on **Reset Times**. After manually changing the start and end times and running a report, this will reset the times to your defaults.

6 The fields of information returned from the history database tables are shown in the **Display Grid**. This information may vary slightly depending on the type of alarm selected. The Query Execution Time at the left hand corner of the screen is simply the time it took for the query to run and return the selected report information. At the right, the First and Last fields are the dates and times of the first and last entries in the database alarm history table.

7 Click **Exit** to close the application.

View Alarm Comments

When an alarm is acknowledged, the operator may enter comments at that time and are what the screen below will display. Additional comments may be added here as shown.

1 Select **File>View Alarm Comments**. The **Existing Commands** section displays the predefined comments for the alarm. You can also double click on an alarm to enter this window.

Options

1 **File>Print Screen** – sends the main screen report information displayed to the printer

2 **File>Display Defaults -** system default times are shown in the dialogue.

Tool Bar

The icon buttons combine the tasks of selecting the alarm type, resetting the time range to the defaults you have set, and running the report. The name of the transaction represented appears in a hint displayed when you pass the cursor over the icon (only the most commonly used transaction types have icon buttons).

Card alarms

Contact alarms

Communications alarms

Controller alarms

Operator alarms

System alarms

Alarm Types

The following are the different alarm types available.

All reports include the following items of information; only relative or additional items will be listed for each report type.

1 **Date and Time** – date and time of the alarm

2 **Transaction** – transaction that generated the alarm

3 **Device –**the device name that generated the alarm

4 **Acknowledged\Secured**- date and time alarm was acknowledged and secured, or 'not secured' if applicable

5 **Area –** the location of the device

6 **Controller** – the controller that the device is attached to.

7 **Acknowledged –** date and time of acknowledgment

8 **Acknowledged By -** user ID of the person who acknowledged the alarm

9 **Cardholder Name –** if applicable, Cardholder's name that used the card or the status of the card (i.e. "card not in database…")

10 **Encoded ID –** from the cardholder badge information

Card Alarms

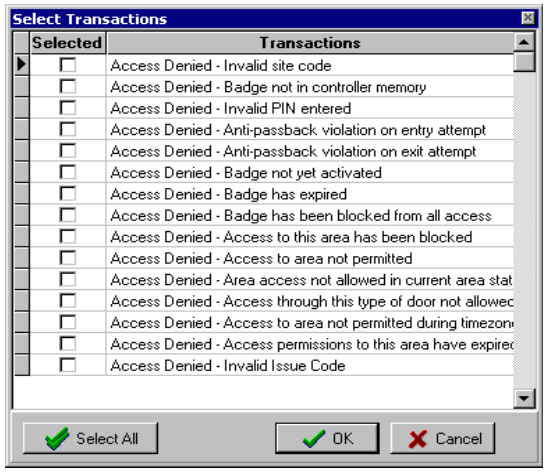
Alarms attached to cardholder transactions are called card alarms.

1 **Access Granted**

- Valid AccessValid Entry
- Valid ExitValid Copy Machine Access

2 **Access Denied**

See the different access denied transactions in the screen capture below.


Select Transactions
Selected
Transactions
Access Denied - Invalid site code
Access Denied - Badge not in controller memory
Access Denied - Invalid PIN entered
Access Denied - Anti-passback violation on entry attempt
Access Denied - Anti-passback violation on exit attempt
Access Denied - Badge not yet activated
Access Denied - Badge has expired
Access Denied - Badge has been blocked from all access
Access Denied - Access to this area has been blocked
Access Denied - Access to area not permitted
Access Denied - Area access not allowed in current area stat
Access Denied - Access through this type of door not allowec
Access Denied - Access to area not permitted during timezon
Access Denied - Access permissions to this area have expire
Access Denied - Invalid Issue Code
Select All
OK
Cancel

Contact Alarms

Alarms attached to contact transactions are called contact alarms.

1 **Contact Transactions**

- Contact Active and Contact Secure

2 **Trouble Open Trouble Short**

3 **Door Forced Open**

4 **Door Held Open**

Relay Alarms

Alarms attached to relay transactions are called relay alarms.

1 **Relay Transactions**

- Relay Energized and Relay Released

Communications Alarms

Alarms attached to the following communications transactions are communication alarms:

1 **Reader Communications**

- Lost Link to Reader

- Restored Link to Reader

2 **Slave Controller Communications**

- Lost Link to Slave RC
- Restored Link to Slave RC

Controller Alarms

Alarms brought about by controller transactions are controller alarms.

1 **Reader Controller Transactions**

- Lost AC Power to RC
- Restored AC Power to RC
- Battery Power Low at RC
- Battery Power Normal at RC
- RC Card Table Full
- RC 75% Full
- Expired Badge Deleted
- Expired Access Privilege Deleted
- Communications Lost to Slave Controller
- Communications Restored to Slave Controller

Operator Alarms

Alarms attached to operator transactions are operator alarms.

- **Workstation -** name of the workstation on which the Alarm occurred
- **Operator -** user ID of the person who was using the workstation when the alarm occurred

1 **Operator Alarm Transactions**

- Logged InOnline Monitor Closed
- Logged OutAlarm Display Logged Out
- System ShutdownAlarm Display Logged In
- System StartupAuto-scheduler Started
- Bad LoginAuto-scheduler Shutdown
- Online Monitor Started
- Alarm Display Logged In
- Alarm Display Logged Out
- Auto Scheduler Started
- Auto Scheduler Shut Down

System Alarms

Alarms brought about by failures of the system process are called system alarms.

1 **System Alarm Transactions**

- CIM Online CIM Lost Link to RC
- CIM OfflineCIM Restored Link to RC
- CIM Started CIM Failure
- CIM ShutdownGather from RC
- Gather RC FailureLoaded RC
- Loading RC Failure Update RC
- Update RC Failure Set RC Clock
- Archiver Started Modified Data Records
- Archiver ClosedHistory Archive Failed
- History Archive CompleteHistory Archive Aborted
- History Archive Started Reader Override

2 Relay Override Contact Override

Guest Alarms

The following guest transactions can be defined as alarms.

1 Guest Pass Transactions

- Guest Signed In
- Guest Authorized

- Guest Signed Out
- Guest REset to Pending
- Guest Deleted Tour System Alarms

Tour System Alarms

1 Tour Operator Transactions

The following are the Tour Operator Transactions that can be defined as alarms.

- Tour Started
- Tour Stopped
- Tour Resumed
- Tour Paused
- Tour Finished with Fault
- Tour Finished Successfully
- Tour Timed Out
- Tour Out of Sequence

2 Tour Reader Transactions

The following are the Tour Reader Transactions that can be defined as alarms.

- Arrived On Time At Reader Checkpoint
- Arrived Early At Reader Checkpoint
- Arrived Late At Reader Check Point
- Reader Checkpoint Never Reached

3 Tour Contact Transactions

The following are the Tour Contact Transactions that can be defined as alarms.

- Arrived On Time At Contact Checkpoint
- Arrived Early At Contact Checkpoint
- Arrived Late At Contact Check Point
- Contact Checkpoint Never Reached

Chapter5:Alarm Graphics-Client

Overview

The Alarm Graphics Client Module connects to the SP and receives alarm transactions. Maps and icons begin to respond to these transactions, based on how they are defined.

In order to receive graphical representation of alarms, the **Alarm Graphics Client** program must be added to the ***Start Up*** tab using **System Security** program. However, the system does not allow you to add both **Alarm Monitor** and **Alarm Graphics** to the ***Start U*p** tab at the same time. So, if you want to add Alarm Graphics program to the Start Up tab, you need to first remove Alarm Monitor from the Start Up.

Note: *The Operator must have at least Read Only permissions to the Alarm Graphics program, in order to see alarms, video or executing override tasks.*

Alarm Notification

When a transaction is generated, and the SP finds an alarm label and attachment that matches the transaction, it generates a new alarm. Based on the alarm label information, the SP sends the alarms to appropriate workstations. To receive alarms in Alarm Graphics Workstation, the administrator has to define one particular computer that runs Alarm Graphics program as workstation, when the alarm labels are defined.

When the Alarm Graphics Workstation receives alarms, the programs searches for icons that have the alarm label attached with it. When it finds the appropriate alarm attachment, it displays the respective map with the animated icon based on the definition, notifying the operator about the state of the alarm (E.G. Unacknowledged and Unsecured).

When a n alarm occurs, the map is displayed showing the animated icon.

See that the icon representing New Jersey state is in red color representing an unsecured and unacknowledged alarm.

Alarm Acknowledgement

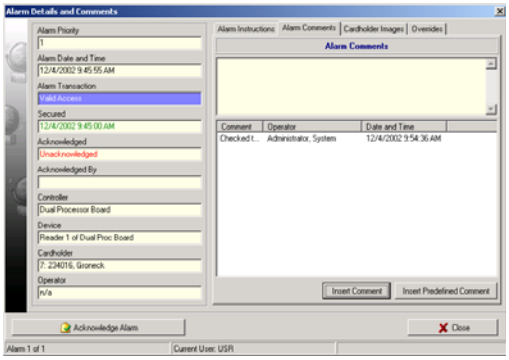
When an alarm occurs, the operator is notified with the graphical representation of the alarm state. Also if there is a sound file attached with the alarm, the system plays the sound file. The operator can access all the possible options from the right click menu of the icon.

The following screen capture shows the right click options available for an Access Granted transaction. These options varies based on the transactions and what options you have set while defining icon definition.

1 **Zoom In:** Click on this option to zoom into another map. This would be the map that is defined as the zoom in map when the alarm goes off.

There can also be a **Zoom Out** map if it is defined in the system.

2 **View Alarm Details:** Clicking on this option opens the **Alarm Details** window. It is here that the operator acknowledges the alarm.



The following information will be displayed in the **Alarm Details and Comments** window.

I. **Alarm Priority:** This indicates the priority level of the alarm.

II. **Alarm Date & Time:** The date and time the alarm has occurred is displayed in this field.

III. **Alarm Transaction:** The transaction that caused the Alarm.

IV. **Secured:** Whether the device that is attached to the particular alarm is secured or not.

V. **Acknowledged:** Whether the alarm is acknowledged or not.

VI. **Acknowledged by:** The name of the operator who acknowledged the alarm.

VII. **Controller:** The controller that is connected to the device which generated the alarm.

VIII. **Device:** The device that generated the alarm. (E.g. In a situation where there is an alarm called "Lost Link to Reader", the Reader is the Device. The name of the Reader will be displayed in this field.)

IX. **Cardholder:** If the alarm is a cardholder alarm, the name of the cardholder will be displayed here.

X. **Operator:** If it is an operator alarm (E.g. illegal login) the name of the Operator will be displayed in this field.

The right hand side of the window contains Instructions to the Operator and the comments that are added by the operator.

Click on the **Alarm Instructions** button to see the instructions to the operator. These instructions are entered in the Alarm Definition program, when an alarm is defined. The administrator can also attach a .wav file with for each instruction.

Depending on how the alarm was defined, you may be required to provide User ID or comments for the highlighted alarm before the system will accept the acknowledgment command. The administrator can "*force login*" and "*force comments*" before letting an operator to acknowledging an alarm. If this is the case, the applicable window will open for you to enter said requirements and acknowledgment will be accepted.

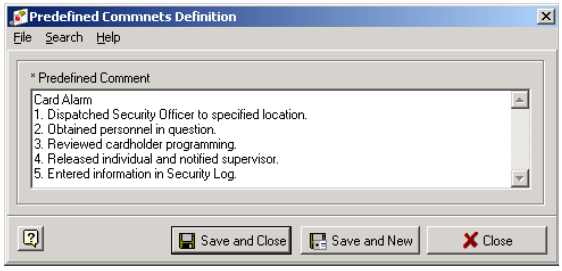
Pre-defined Alarm Comments

While entering comments you have the option to select the predefined comments or enter comments free- form.

Geoffrey System provides a program for the Administrator to set pre-defined comments for the operator to enter while acknowledging the alarms. Follow these steps to define alarm comments.

1 Open the **Pre-defined Alarm Comments** program from the System Launcher.To add new set of comments, click on the plus sign in the **Pre-defined Comments** window.

2 Enter the comments in the **Pre-defined Comments Definition** window.



3 Click <**Save and Close**> to save the application and return to the main window. Click <**Save and New**> to save the current definition and define a new one. Click <**Close**> to close the Definition window with out saving the defined comments.

4 While defining alarms, the administrator can attach these comments with the alarm. The operator shall be able access these comments from the **Alarm Details** window while acknowledging the alarms.

5 **Receiving Video of Alarms**

If there is Geoffrey Digital Video Transaction Retrieval System attached to your Geoffrey Access Control System, you can receive video of each transaction that occurs in the system. The Alarm Graphics program is capable of displaying live and recorded video. The recorded video is displayed in a separate window so that the user can still receive the live video while viewing the recorded video.

I You can play the video by right clicking and selecting *Live Video* option on the icon located on the map.

II You can also access the video from the **Alarm Details and Comments** window under **Live Video** tab.

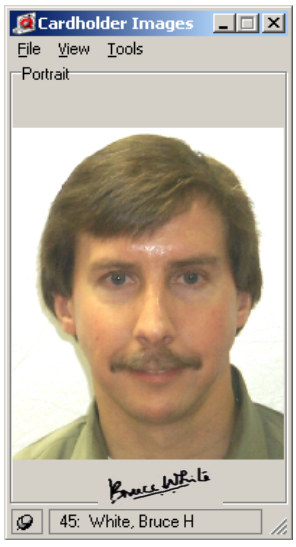
Note: *In order to receive live and recorded video of transactions in the Alarm Graphics System, you should have GVTR system attached with the Access control System. The user also should define cameras while defining the icons.*

III. In the **Alarm Details** window click on the button **Live Video**. The video from the camera associated with the transaction will be displayed on the screen.

IV. Click on the **View Recorded Video of this Alarm** button to play back the video of the alarm. This video file is opens in a new window called **GVTRPlay5** so that display of live video is not interrupted.

View Cardholder Image

Click on the button **Cardholder Images** from the **Alarm Details and Comments** window. The cardholder portrait and signature are displayed.

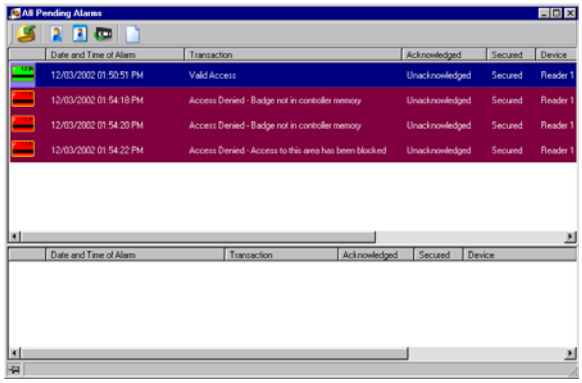


1 Preview Pending Alarms on this Icon

You can also view all active alarms that are routed to Alarm Graphics workstation. When you click this option these alarms (alarms for the selected icon only) will be displayed in Pending Alarms window.

Double click on these alarms to acknowledge them. The Alarm Details and Comments window is displayed.

You can also access the Alarm Details window from the right click menu of the alarm or the tool bar icon.



2 Find Alarm in the All Pending Alarms

When you click this option, the system highlights the alarm that you are viewing in the **All Pending Alarms** Window.

3 Executing Override Tasks

When an alarm occurs, the operator can execute necessary actions using the Override Tasks that are defined in the system. Each icon can have any number of manual override tasks associated with it.

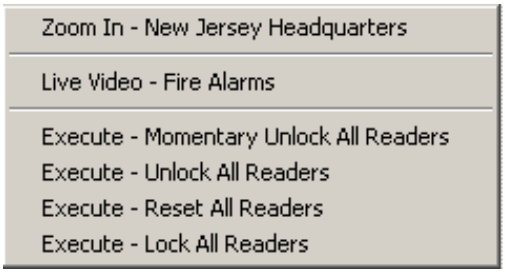
- Select and click on the task that you want to execute. The override task will be executed as defined in the Manual Override Definition program.

Default State of an Icon

The operator can access different available options like live video, override tasks etc. while the alarm is in the default state i.e when there is no alarm in the buffer.

The user is also capable of accessing other maps depending on how icon is defined.

Right click on the icon to see the options that are available for the icon.


Zoom In - New Jersey Headquarters
Live Video - Fire Alarms
Execute - Momentary Unlock All Readers
Execute - Unlock All Readers
Execute - Reset All Readers
Execute - Lock All Readers

These options may vary depending on how they are defined.

Links to other maps in the system, zoom out map etc. are some of the possible options.

Search for Icons and Maps

Alarm Graphics workstation is equipped with search feature for easily locating icons and maps especially when you have large number of items defined in your system.

1 Select **Find>Map** or ***Icon*** from the **Search** menu.

You can also access these by clicking on the respective tool bar icons that are available in the main tool bar of the program.

2 The **Search** window is displayed. Enter the name of the map or icon that you are looking for. Remember that you don't have to enter the name completely. If you enter the starting letters of the map, the system finds all the maps beginning with those words.

You can also put wild cards (percentage sign %) with the letters you are entering to find the maps or icons that contains those letters.

Use of Wildcard

The search feature provides ways to select certain records without typing complete information. Geoffrey System allows the use of wildcard (more formally known as *metacharacters*) to stand for one or more characters in a record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the % (percent sign) as a **wildcard**. Within the search criteria, a user can type the % character as a wildcard before or after their search text.

Advanced Find

Using Advance Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

Maps and Icons can be searched using fields like map ID, caption etc.

1. Click on the Advanced Find tab located on the top of the Search window.
2. The Advanced Find window opens.
3. To define the criteria, select the field name, condition and value. At least one criterion must be selected for the feature to work properly. When you run the search you will get the records corresponding to your search criteria.
4. Once you have defined the criteria click **File>Save**.
5. Add a description to your search and click **OK**. The new search will be saved and listed under the Advanced Find button.

Chapter6:Transaction Monitor

Introduction

Transaction monitor does a real time display of cardholder and device transactions. The user can set filters for certain transactions and save each Transaction Monitor separately. The user can screen out unwanted information by doing this. The program also allows the user to open multiple monitors simultaneously at the same workstations. With proper authorization, the user can access the Cardholder Definition, Previous Transactions and Transaction Filter Modules from the Transaction Monitor program as well. This enables the user to view Previous Transactions in one window while another window shows ongoing activity.

Accessing the Application

1 Double click the System Launcher icon from the desk top.

2 Enter your assigned user id and password in the Login window.

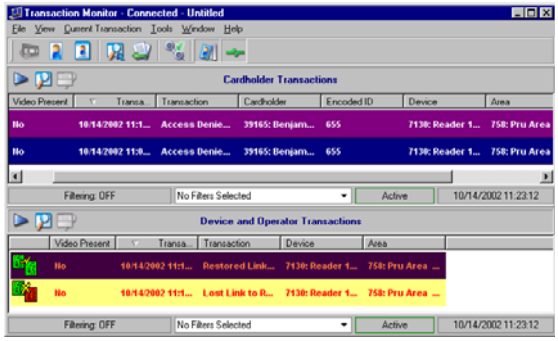
3 In the System Launcher window, select the Transaction Monitor icon and double click on it.

Overview

Transaction monitor window is divided into two panes. The upper pane displays Cardholder Transactions and the lower pane displays Device and Operator Transactions. The user can also view cardholder portraits and signatures for verification. In addition to that the User Defined Fields are also displayed in column, if they have been selected in the User Defined Fields Editor.

Using the Transaction Codes program all the transactions can be customized by font color, size, style, name and background color.

Note: *The operators must have appropriate permissions to open the Transaction Monitor. Refer to the System Security chapter for further details.*



Working with the Transaction Monitor

Defining a Monitor

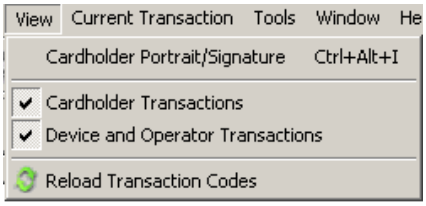
Customize the Transaction Code

The first thing the user must do before defining the Transaction Monitor is, customizing the color schemes for different transactions in the Transaction Codes Editor.

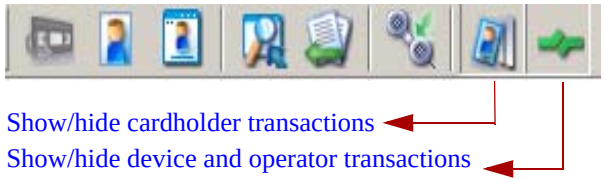
1. Open the Transaction Codes program and select the transaction you want to customize and double click on it.
2. In the Transaction Codes Editor window, there is a section named Transaction Code Display Information. Customize the Transaction Code by selecting a font color, size, style, name and background color appropriate for the particular transaction.
3. Select **File>Save and Close** to save the definition. Like this you can customize each transaction you have.
4. In the Transaction Monitor Program select **View>Reload Transaction Codes** to view the transactions in the newly defined style. Otherwise the Transaction Monitor must be closed and reopened to display the new style you have defined.
5. Customizing the Transaction Monitor

Selecting the Transaction GroupI

n the Transaction Monitor window the user can either select to viewCardholder Transactions only or Device and Operator Transactions only or both.



You can also choose to show/hide transactions by clicking on the tool bar icons.



Pausing Transactions

You can always stop the transactions being displayed in the transaction monitor by enabling the pause option.

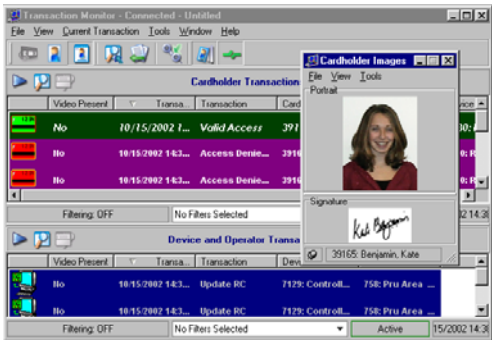
There are separate options for pausing cardholder and device and operator transactions. This helps the user to stop one particular transaction while the other continue to display.

1. Select **Fie>Pause Cardholder Transactions** to stop only cardholder transactions being displayed.
2. Select **Fie>Pause Device and Operator Transactions** to stop all the device and operator transactions being displayed.

Viewing Cardholder Portrait and Signature

If you are viewing Cardholder Transactions you can choose to view the Cardholder Portrait or Signature to reassure the security further.

1. Select **View>Cardholder Portrait** or Signature.



2 If you want to verify only the cardholder image, deselect **View>Signature** from the Cardholder Images dialogue.

3 If you want to verify only the cardholder signature, deselect **View>Portrait** from the CArdholder Images dialogue.

4 Selecting **View>Clear Images** option removes the images from the window.

5 To snap the Cardholder Images winodw to the corner of the computer screen, select **Tools>Options**. On the **Cardholder Images Preview Settings** window, select the ***Snap Cardholder Images Window*** checkbox and adjust the value using the up and down arrows.

6 To close the image preview dialogue, select **File>Close**.

You can also show/hide the portrait/signature preview window by clicking on the tool bar icon.

Show/hide portrait and signature preview window

Playing Video File of a Transaction

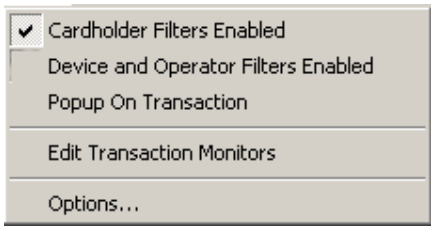
7 Select **Current Transaction>Play Video** to view the video of a transaction.

Filtering Transactions

The user can enable filters for cardholder or device and operator transactions or both. This feature allows the user to screen out unwanted transactions from the monitor.

There are separate filters for Cardholder and Device and Operator Transactions.

8 If you want to enable filters for Cardholder Transactions only select **Cardholder Filters Enabled** option. A check mark appears indicating that you have enabled that option.



9 If you want to enable filters for Device and Operator Transactions select the option **Device and Operator Filters Enabled**.

10 Double click on the **Filtering On** button from the upper or lower pane depending on the type transactions you want to filter out. All the transactions corresponding to that group will be displayed. Select the transactions you want to filter and click **OK**.

Now only the transactions meeting these selected filters will be displayed.

Note: *All the grids and columns that appear on the Transaction Monitor window are resizable and sortable.*

Popup on Transaction

If you select *Popup on Transaction* option from the **Tools** menu the Transaction Monitor window will pop up automatically whenever a transaction occurs.

Note: *Double click on the transactions to get an info-tip showing all the information of the selected transaction*

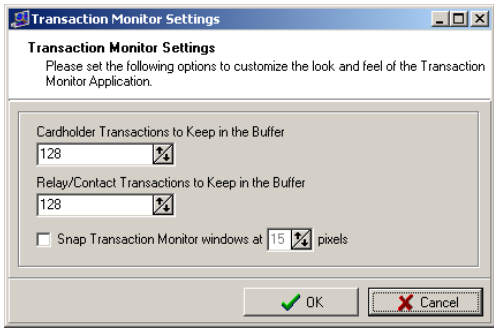
Auto-load the Saved Monitor

While saving a monitor you can set the option to auto-load the saved monitors when the Transaction Monitor program is first opened. Instead of opening an untitled monitor the program will open the monitors that you have saved as auto-load.

Options

The user can further customize the monitors by setting the number of transactions to be displayed on each Transaction Monitor that is saved.

1 Click **Options** from the **Tools** menu. The following window is displayed.


Transaction Monitor Settings
Transaction Monitor Settings
Please set the following options to customize the look and feel of the Transaction Monitor Application.
Cardholder Transactions to Keep in the Buffer
128
Relay/Contact Transactions to Keep in the Buffer
128
Snap Transaction Monitor windows at 15 pixels
OK
Cancel

2 Enter the number of transactions you want to be displayed in the monitor.

3 You can also specify the number of pixels at which the Transaction Monitor window snaps to the corner of the screen.

Saving Transaction Monitors

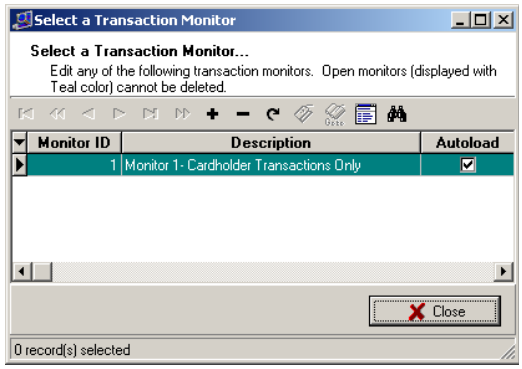
Once you have customized the monitor according to your needs, you can save it by giving a unique name. Like this you can define as many monitors as you like and save them separately. The system also supports multiple document interface which allows the user to open more than one transaction monitor at a time. All the saved monitors are protected by the operator login and those won't be available for another user.

Each saved monitors can have the following options saved.

- Viewing either Cardholder Transactions or Device and Operator Transactions or both.
- The filters enabled.
- Cardholder image is displaying or not.
- The option to pop up the transactions.
- Auto-load the saved monitor when the Transaction Monitor program is first opened.
- Set the number of transactions displayed.

Editing Transaction Monitors

1 Select **Edit Transaction Monitors** from the **Tools** menu.

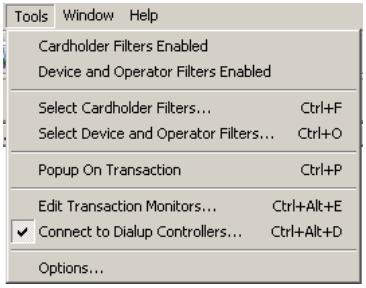


2 Double click on the monitor you want to edit. The monitor you have selected is displayed for editing.

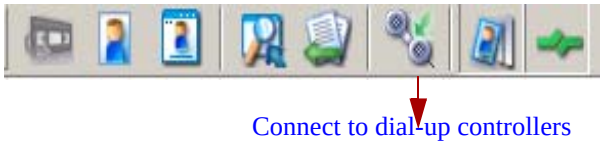
Connecting to Panels via Dial-up

Transaction Monitor program allows the user to connect to the controllers located at remote locations using a dial-up modem and get transactions.

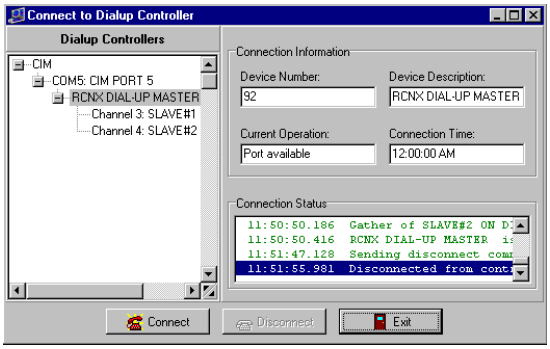
1 Select Connect to Dialup Controllers from the **Tools** menu.



or click on **Connect to the dial-up controllers** icon to select the device.



2 The following window is displayed.



3 Select the Device and click **Connect**.

The CIM dials the controller specified and gets the recent transactions.

Pausing Transactions

Select the **Pause Cardholder/Device and Operator Transactions** from the **File** menu to temporarily either of the transaction types displayed in the Transaction Monitor.

Viewing Previous Transactions

1 Select **View Previous Transactions** option from the **File** menu.

2 Enter the transaction type, day that transactions occurred, start and end time of the transactions etc.

3 Click on the **<Run Report>** button to run a report of the transactions you selected.

Accessing Other Applications From Transaction Monitor

Cardholder Definitions

You can access Cardholder Definition program from the Transaction Monitor to view or edit cardholder records pertaining to the transactions.

Select the **Cardholders in Cardholder Definition** from the **Current Transactions** menu.

Transaction Filters

You can access Transaction Filters program from the Transaction Monitor.

1 Select **Edit Transaction Monitor Filters** from the **File** menu.

Chapter 7: Previous Transactions

Introduction

The View Previous Transaction module will provide an account of any transactions in the database. You can select which transaction type you want to view, the date, time and the sorting order to be displayed.

Accessing the Application

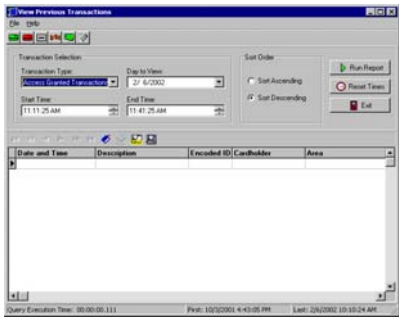
1 Open the Geoffrey Launcher by double clicking the Launcher icon on your desktop.

2 The login window, opens. Enter your user id and password.

3 In the System Launcher window, double click on **Previous Transactions** icon.

Overview

The main screen consists of the menu and tool bars, transaction selection, sort order and report controls, display grid, navigation bar, and status bar. Details follow for all screen features.



Running a Transaction Report

1 First select the **Transaction Type** from the drop down list. Drop down menu offers all system Transaction Groups to choose. You can only choose one transaction type at a time

2 Next choose the **Day to View**. By default it will be the current date. To change this, click on the down arrow to open the calendar. A red circle will appear around the current day.

3 Now set the **Start Time**. The default is set until you change it. To change this manually for the current report, click on the hour, minute, or second to highlight it and use the up and down arrows or type in the field.

Note: *When you change the start time manually, the end time will set to 11:59:59 PM and has to be changed manually if necessary.*

4 Set the **End Time**. The default is set at the current time. Changes are made the same as with Start Time. Select **File>Display Defaults** to change the defaults for the current reporting time periods. The system defaults are set to: Start 30 minutes prior to current time and End at current time, shown below.

5 Specify the **Sort Order**. Choose ascending or descending.

6 Click **Run Report** to begin the report. The fields of information returned from the history database tables are displayed in the **Display Grid**. This information may vary slightly depending on the type of transaction selected.

7 **The Reset Times** button resets the time to the default you have defined

8 Click **Exit** to closes the View Previous Transaction window.

Note: *In the **Status Bar** the Query Execution Time at the left is simply the time it took for the query to run and return the selected report information. At the right, the First and Last fields are the dates and times of the first and last entries in the database transaction history table.*

Printing the Screen

1 Select **File>Print Screen** to send the current screen to designated printer.

Tool Bar Items

Only the most commonly used transaction types have icon buttons. For more choices, use the Transaction Type drop down menu.

Note: *When you click on one of these buttons, the Start and End time will be reset to the default, any current display will be cleared, and transactions occurring within the default start and end time will be reported immediately.*

(In order of appearance from left to right)

- Access Granted
- Access Denied
- Reader Communications
- Contact Transactions
- Reader Controller Transactions
- Operator Actions

Transaction Type Definitions

There are several Transaction Types available to choose from. Descriptions of them follow.

Note: *As the list progresses, we will only detail differing items of information for each group.*

Access Granted Transactions

Transactions include valid access, entry, exit and copy machine access. The report returns the following information:

I. **Date and Time** - of the transaction – returned for all transaction types

II. **Description** - the transaction that took place – returned for all transaction types

III. **Encoded ID** - the encoded ID number of the card used in the transaction (This can only be seen if the operator has permission to view encoded ID numbers.)

IV. **Cardholder** - the name of the person ID card is assigned to

V. **Area** - location transaction occurred in – returned for all transaction types

VI. **Controller** - the defined name of the Controller that reported the transaction

VII. **Device** - the defined name of the Reader on the Controller that reported the transaction

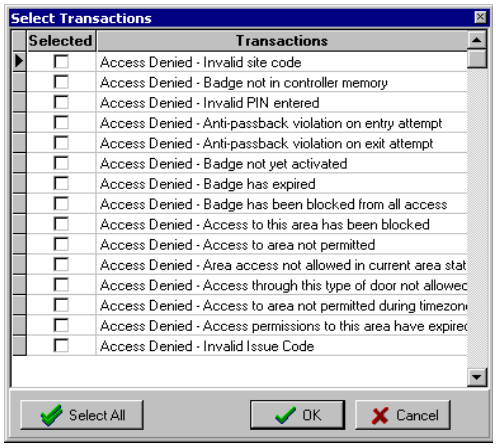
Archive History

This displays Archiver transactions and status.

Note: *Current versions of Geoffrey Access Control do not implement this feature.*

Access Denied Transactions

Transactions include all those found in the Access Denied group.


Select Transactions
Selected
Transactions
Access Denied - Invalid site code
Access Denied - Badge not in controller memory
Access Denied - Invalid PIN entered
Access Denied - Anti-passback violation on entry attempt
Access Denied - Anti-passback violation on exit attempt
Access Denied - Badge not yet activated
Access Denied - Badge has expired
Access Denied - Badge has been blocked from all access
Access Denied - Access to this area has been blocked
Access Denied - Access to area not permitted
Access Denied - Area access not allowed in current area stat
Access Denied - Access through this type of door not allowec
Access Denied - Access to area not permitted during timezon
Access Denied - Access permissions to this area have expirec
Access Denied - Invalid Issue Code
Select All
OK
Cancel

Reader Communications

This reports any disruptions or restorations in the communications between the Reader Controller and the Reader interface. The report returns the following:

- **Description** – Lost or Restored link transactions
- **Reader** - the defined name of the Reader on the Controller that reported the transaction

Contact Transactions

These are specific changes detected in the normal monitored state of an input (i.e. motion detectors, doors, etc.). The report returns:

- **Description –** the transactions relate to contact points only.
- **Contact** - the number of the contact on the reader controller that reported the transaction, and the description of the device, typically the location of the contact point

Slave Controller Communication

This option reports on the status of the connections between the Master Controller and the Slave Controllers. The following information is returned:

- **Description** – Lost or Restored link transactions
- **Controller** - the defined name of the Slave controller board

Reader Controller Transactions

This displays status messages originated by the Reader controllers. The report contains the following:

- **Description -** of controller occurred during the transaction

Operator Transactions

This gives a report of the system activities of defined Operators and the workstations that they are using. These items are returned:

- **Description** - Operator activity on the system
- **Operator** - the user ID of the person using the workstation
- **Workstation** - the name of the workstation

CIM to RC Communications

Transactions relating to communications between the CIM and the attached Reader Controller are returned. The Reader Controller will store information on expired badges and access records for 48 hours after expiration for the purpose of advanced notice prior to record deletion. These two types of transactions are newly included in this group.

CIM and SP Status Messages

This option displays transactions involving the status of the CIM or SP. The information includes:

- **Workstation** - which workstation the message came from

Download/Update Status Messages

These transactions are related to system information downloads or updates from the CIM to the Controller.

- **Description** – Reports whether update or download was sent to the reader controller

Device Control

This option relates to transactions during which an operator performs any type of Manual Override to a specific device.

Note: *Current versions of Geoffrey Access Control do not implement this feature.*

Guest Pass Transaction

The transactions occur while using the Guest Pass System is called Guest Pass Transactions. The following is the list of transactions.

- Guest Signed In
- Guest Authorized
- Guest Signed Out
- Guest Reset to Pending
- Guest Deleted Tour System Alarms

Security Tour System Transactions

1 **Tour Operator Transactions**

The following are the Tour Operator Transactions that can be defined as alarms.

- Tour Started
- Tour Stopped
- Tour Resumed
- Tour Paused
- Tour Finished with Fault
- Tour Finished Successfully
- Tour Timed Out
- Tour Out of Sequence

2 **Tour Reader Transactions**

The following are the Tour Reader Transactions that can be defined as alarms.

- Arrived On Time At Reader Checkpoint
- Arrived Early At Reader Checkpoint
- Arrived Late At Reader Check Point
- Reader Checkpoint Never Reached

3 **Tour Contact Transactions**

The following are the Tour Contact Transactions that can be defined as alarms.

- Arrived On Time At Contact Checkpoint
- Arrived Early At Contact Checkpoint
- Arrived Late At Contact Check Point
- Contact Checkpoint Never Reached

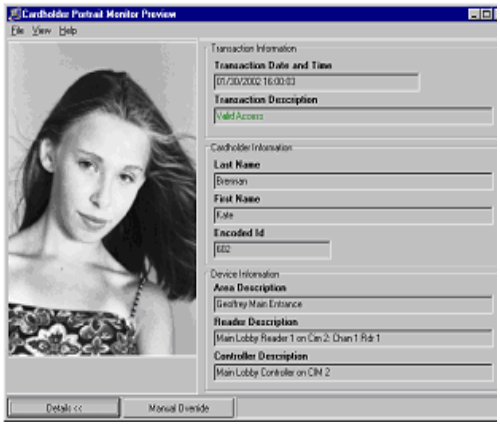
Relay Transactions

- Relay Energized and Relay Released

Chapter8:Portrait Monitor

Introduction

Geoffrey Access Control System offers another type of reporting tool, the **Portrait Monitor** module. Activity and images are viewed instantaneously on any designated computer monitor. This application can be used to validate and track cardholder identity and access. Detailed information with cardholder or guest images is examined as the transaction occurs. Assigning workstations as portrait monitors is accomplished in the **Portrait Monitor Control** module. See Geoffrey Administrator Manual for further details.



Starting the Portrait Monitor

This module can be added to the **Start up** tab in the **System Security** program for each workstation that is to receive alarms.

1 To do this, go to **System Security\Startup**, click **Add** and select Portrait Monitor.

Note: *Remember to give proper privileges (at least Read-Only rights) to the users of Portrait Monitors or they will not be able to use the program.*

You can also open the program from the System Launcher window.

1 Open the Geoffrey Launcher by double clicking the Launcher icon on your desktop.

2 The login window, opens. Enter your user id and password.

3 In the System Launcher window, double click on **Portrait Monitor** icon.

Overview

The main screen components of the application are the menu bar, the image view section to the left, the details information display to the right (on by default) and manual override and details buttons at bottom left.

Working with the Portrait Monitor

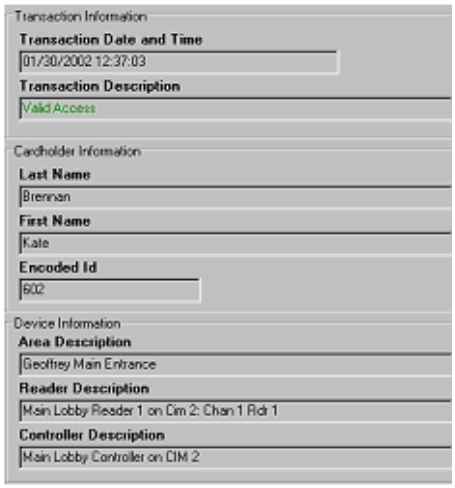
Launching the Portrait Monitor

1 Select **View>Popup Enabled** option to launch a minimized Portrait Monitor screen when a transaction occurs.

Detail View

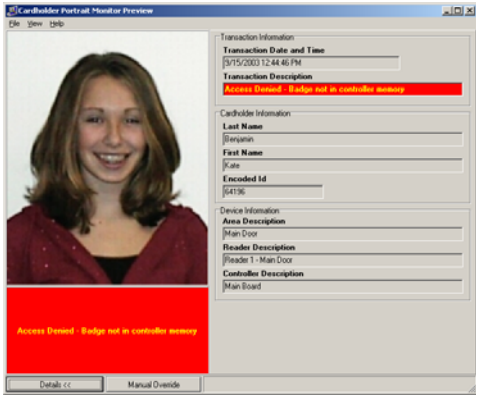
The **Details** section displays the transaction information, cardholder information, and the device information.

1 Select **View>Details** to turn on the detail information section. (on by deafult). When **View>Details** is unchecked only the **Image View** (cardholder's portrait view) is active and therefore no transaction, cardholder or device information is seen. The Details button at the bottom functions in the same way.



Access Denied Transactions

In the Portrait Monitor, Access Denied transactions are displayed in red color. When an access denied transaction occurs, a red panel displays underneath the image stating the transaction. The user can resize this field to their convenience and it will save to the User Registry when the program is next opened.



Pausing Transactions

1 Select **View>Pause** to halt the application temporarily from displaying any new transaction. The information that was on the screen at the time that **Pause** option was selected will remain.

Manual Overrides within Portrait Monitor

Clicking **Manual Override** located at the bottom of the Portrait Monitor window opens the main window of the Manual Override module. Provided that the operator has at least *Read Only* rights to the Manual Override module, he can execute a device override. Highlight the task and select the Execute Override Task button. Please refer to the **Manual Override chapte**r for further information on this module.

Chapter9:Audit Trail Report

Introduction

Audit Trail Report is a program that allows you to conveniently monitor any additions, deletions and changes made to your database. This module is used to create reports and view differences in the data tables. Virtually all Area Access, Area, Cardholder, Badge and Time zone information can be organized and viewed.

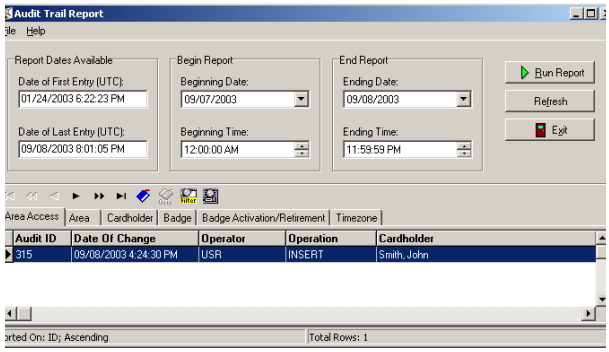
For example, if an operator mistakenly deleted an Area that in turn affected cardholders and their Area Access, you can quickly determine which user was responsible, the date of the change, the Area name, the original value and the updated value.

Accessing the Application

1. Open the Geoffrey Launcher by double clicking the Launcher icon on your desktop.
2. The login window, opens. Enter your user id and password.
3. In the System Launcher window, double click on **Audit Trail Report** icon.

Overview

The Audit Trail Report window displays three categories with sub-fields that need defining. They are **Report Dates Available**, **Begin Report** and **End Report**. These fields set the parameters of your Audit Trail Report.



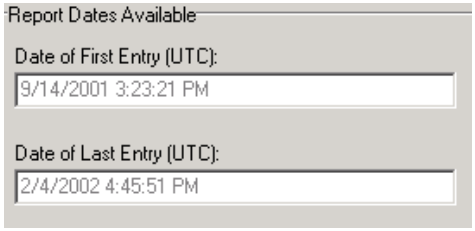
In the Audit Trail Control module, the "**Duration of History**" option determines the amount of data that is stored in the system. After the amount of days specified, the records are deleted from the Audit Trail tables. If the duration is set to 14, that indicates you will not be able to create a report that includes data beyond the 14 day range regardless of what is entered in the **Beginning Date** and **Ending Date** fields of the Audit Trail Report module.

Generating a Report

In order to generate an audit trail report you need to specify the following fields in the Audit Trail Report program.

Report Dates Available

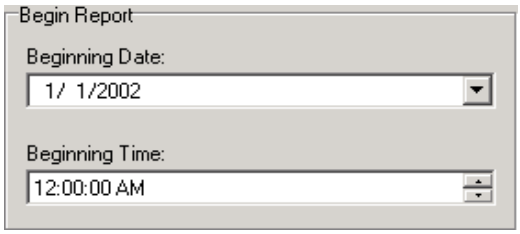
The first category is called Report Dates Available. This has two fields, Date of First Entry (UTC) and Date of Last Entry (UTC). These fields represent the absolute limits of your date definitions;obviously you cannot ask for reports of changes in your database before it was installed or beyond today's date. Therefore, you are limited to the period of time between these two dates as listed in the fields.



Begin Report

Begin Report has two fields. You can set the extent of your report by defining in the **Beginning Date** field the exact day from which you want to check all system activity, though the default is today's date. You further clarify this with the next field, **Beginning Time**, which defaults to 12:00:00 a.m.

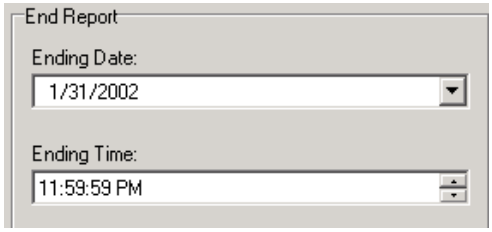
Note: *It is important to remember that the number of days you set in the* ***Duration of History*** *(in Days) in the Audit Trail Control module will dictate the absolute limits of when you can gather records. If you set the duration for 14 days, a Beginning Date before 14 days from today is invalid because all auditing records beyond 14 days have been deleted.*



End Report

End Report allows you to delineate the utmost time limits that your report will collect information. In other words, it determines the last day to be included in your report. Both the Ending Date and Ending Time field define it.

The Ending Date field defaults to the current date, but this can be changed to an earlier date if you want to define a specific time period (for example, a Beginning Date of January 1st to an Ending Date of January 15th. The Ending Time field defaults to 11:59:59 pm but this can also be changed to your specifications.



Run Report

After all the categories are defined, click the Run Report button on the upper right side of the window and it will gather information from the system and organize the report along your specifications.

Refresh Report

When you change any of the criteria of the fields , click the Refresh button to generate new data.

Understanding a Report

After a report has been run, the information captured from your Geoffrey database will be displayed in column and grid format on the bottom of the screen. This information in the grid display can be viewed six different ways, each represented by a tab. These tabs are: **Area Access**, **Area**, **Cardholder**, **Badge**, **Badge Activation/ Retirement**, and **Timezone**.

The fields are displayed in grid format under the selected tab. One record created in the Cardholder Definition module can easily result in ten to fifteen rows displayed on the Audit Trail Report.

Note: *Each individual record you create, such as a cardholder, has many fields that can be monitored by the Audit Trail Report. Whereas you may have created only one Cardholder, the Audit Trail Report can display all fields associated with that record, such as First Name, Last Name, Cardholder ID, etc. as shown in the following examples.*

Each tab in the Audit Trail Report represents a Table. Many of the columns titles, which mirror fields of your records, are found in more than one tab.

Click on each tab to see the corresponding database changes that are made. The report shows data of change, the operator's user id, activity (insert or update), and cardholder's name.

Column Name Definition

I. **Area**: This lists the Area description as defined in the software.

II. **Audit ID**: This is the number assigned by the system to the specific record field (entire row) in the context of the whole Audit Trail Report.

III. **Cardholder**: This displays last and first name of the cardholder.

IV. **Column Name**: The actual title of the field that was created, changed or deleted such as CardholderID.

V. **Data Table**: This defines the table name where activity was recorded in the Geoffrey software. If a badge was activated or retired, the table name will display in the Data Table column of the Badge Activation/Retirement tab.

VI. **Date of Change**: This reflects Date and Time of inserts or updates that were made.

VII. **Encoded ID**: This is the unique number assigned to a cardholder's badge. This number is physically programmed into the badge and is read by the reader and used to identify the cardholder and their access privileges.

VIII. **Operator**: This shows the User Login name that made the change.

IX. **Operation**: This column lists they type of activity that occurred in the database. *Insert* will be listed when any new records have been added; *Update* is listed when you have altered an existing record and *Delete* indicates that an operator has removed record.

X. **Original Value**: This will list initial properties of the record you are viewing. For newly created records (Insert), the Original Value will be blank.

XI. **Updated Value**: This shows whatever modifications have been made to pre-existing records. You can use this to compare the new Updated Value with the previous value given to the record, which is shown in the **Original Value** column.

XII. **Referencing Timezone**: This is the name of the Timezone that was deleted.

Rearranging and sorting Column Titles

Column titles can be placed in any order that is convenient to the user. Simply drag the column title and drop it to a new location. To sort in ascending or descending order, click in the title bar.

The sort order is viewed on the bottom, left of the screen. Total Rows is written to the left of the sort order.

Chapter10:Report Launcher

Introduction

The Report Launcher module allows operators with the proper security privileges to create, add and generate comprehensive reports. The Geoffrey software provides report groups for Alarm History, Archive History, Audit Trail, Cardholders, Database, Guest Pass, History, and Transaction History reports. Report wizards make the creation and output format fast and simple. You may print and/or export reports to other applications, store to disk or send to mail recipients, as well.

The Report Launcher is used to generate reports that contain specific criteria. All available reports reside under a group name in the Report Tree. There are seven Report Groups; they are Alarm History, Archive History, Audit Trail, Cardholder, Database, Guest Pass and Transaction History reports. Additional Report Groups and reports can be created in the Report Settings module.

The main window contains the Menu bar, Shortcut icons, Quick Launch drop down option and the Report Tree.

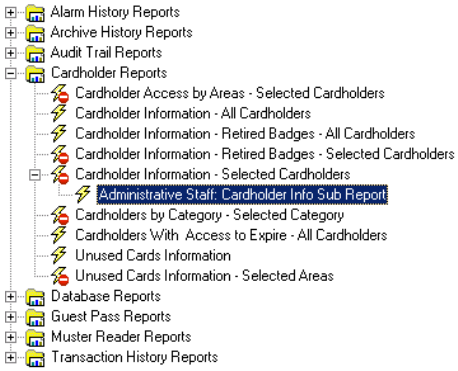
Accessing the Application

1. Open the Geoffrey Launcher by double clicking the Launcher icon on your desktop.
2. The login window, opens. Enter your user id and password.
3. In the System Launcher window, double click on **Report Launcher** icon.

Overview

Report Tree View

The Report Tree displays Report Groups with it's associated Base, Derived and Derived Sub-reports that can be generated. Base reports are predefined Geoffrey reports. Derived reports are used to create sub-reports; they are represented by a yellow, lightning bolt with a red circle. Derived Sub-reports and Base reports can be launched immediately and will have a icon.


Alarm History Reports
Archive History Reports
Audit Trail Reports
Cardholder Reports
Cardholder Access by Areas - Selected Cardholders
Cardholder Information - All Cardholders
Cardholder Information - Retired Badges - All Cardholders
Cardholder Information - Retired Badges - Selected Cardholders
Cardholder Information - Selected Cardholders
Administrative Staff: Cardholder Info Sub Report
Cardholders by Category - Selected Category
Cardholders With Access to Expire - All Cardholders
Unused Cards Information
Unused Cards Information - Selected Areas
Database Reports
Guest Pass Reports
Muster Reader Reports
Transaction History Reports

Report Groups

Under every Report Group in the tree are base and derived reports and any predefined (user created) sub-reports. New report groups can be added using the Report Settings application.

Base Reports

These reports are predefined in the Geoffrey software and therefore need no further user input except a Date and Time selection. Base Reports can be immediately launched and are indicated by a yellow lightning bolt. An example of this type of report is the Cardholder Information Report – All Cardholders. Since all cardholders are reported, it is not necessary for the user to select any cardholders.

Derived Reports

Derived Reports are identified by a lightning bolt with a red circle. They cannot be launched. Instead they use Base report criteria and require selections to be entered that define a user created sub report. Some examples of selections are cardholders, areas, readers, relays and contacts.

Derived Sub Report (User Created)

The plus sign next to a Derived icon in the Report Tree indicates that a user created sub-report has been defined and is available. Expand the tree and the report will have a icon.. This type of report is created by highlighting a Derived Report, choosing **Create New Report** and supplying information in the New Sub Report Wizard. Once defined, it can be launched and will use the selections made in the wizard for the result set. No other operator will be able to launch, delete, or edit these reports except for the operator who created it

Note: *The yellow, lightning bolt icon means that the report can be launched immediately.*

Launching a Report

In order to launch a report, there must be a yellow, lightning bolt graphic next to the description. This is the indication that the report will generate.

1. Highlight the description within the Tree and click the **Launch Report** button or right click and send the command from the sub menu or select **File>Launch Report**.
2. If a Date and Time is required, an entry dialog will appear. Once this information is entered, the report will be displayed in its own window.

Quick Launch Feature

The Quick Launch feature makes it easy to run recently launched reports. By default, it keeps track of the last ten reports that have been launched (not using the quick launch).

You can then easily use the drop down list in the combo box to select one of these reports and launch it by clicking the yellow, lightning bolt button to the right of it. You will also find a list of these reports under **File>Recently Launched Reports**.

Printing and Exporting Reports

Printing

1. To print a report, just click on the printer icon shown in the toolbar of the report output display screen. The default Windows printer selected will be used here. The print range, collate option and number of copies may be selected.

Exporting

Also located on the toolbar is the Export button, which will open the Export window. This feature allows you to choose a format and destination for exported reports. The format and destination choices for these files are specific to the applications you have installed as well as the version of Crystal Reports.

Adobe Acrobat, Word for Windows and Excel files are among several file types supported by this Crystal Report utility.

Note: *Geoffrey access control system verrsion 5.1.4 do not support formats like Character seperated values, Crystal 7.0, Data Interchange Format DIF, Various Versions of Excel, Lotus selections, ODBC and Paginated Text.*

Creating a New Sub Report

Creating a new report is easy. Simply click on the appropriate Derived Report (indicated by a lightning bolt with red circle). For example, if you want to run a cardholder information report on only a few cardholders, select the Cardholder Information Report - Selected Cardholders.

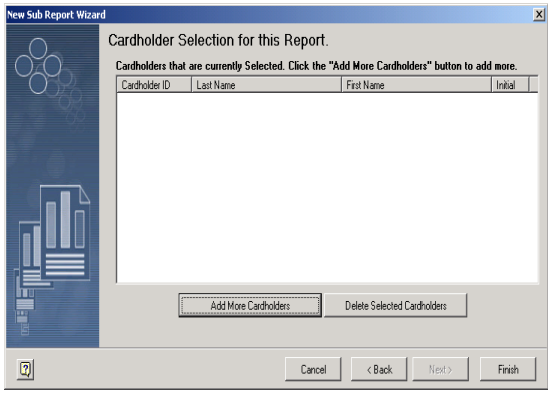
1 Once you have highlighted the appropriate report, click **Create New Report** or right-click on the highlighted report, and select **Create New Sub Report**. You can also start the wizard by double-clicking the derived report. When you click the button, the New Report Wizard will display. Step through this wizard until all of the appropriate selections have been made. The wizard will not let you finish until all of the required data has been entered or selected.

2 The first step of the wizard is to enter the Description and Notes of the report. The description is displayed in the tree and helps you remember what the report is. You have 64 characters of space for this field, which is enough for a good description. Remember, the base report also has a description, which further defines what this new report is. If you need a very elaborate description, you can use the Notes field, which allows 255 characters.

3 Lauch this Report after it is created option allows you to immediately begin to run the report using all of the criteria you have selected in creating it.

4 The remaining steps of the wizard will ask you to select one or all of the following: Cardholders, Areas, Categories, Readers, Relays, Contacts, Controllers, CIM Ports, CIMS, and Workstations.

For example, for a selected cardholder report, you would see the following page:



This page is asking you to add cardholders to the report. These cardholders will be used as the data for the report.

5 When you click **Add More Cardholders**, the Cardholder Search wizard will display. The Cardholder Search wizard allows you to search for cardholders within the database and select them. You must type in all or part of the last or first name and then hit the enter key. The cardholders that match the search criteria will be displayed on the bottom. Use the Find Now button to see the entire list of cardholder.

6 Highlight cardholders (holding the CTRL key as you click) and hit the enter key or choose **OK**.

These cardholders will be selected for the report and will show up in the initial selection wizard screen. All of the cardholders that are displayed in this screen will appear in the report.

7 Click **Finish** to launch the report. If the Launch Immediately button was checked in the first step, the report will be launched automatically.

Note: *The method of selecting Devices and Areas is a little different, but easy to use and follow. You will see these steps only if the report requires those selections.*

Editing a Sub-report

1 In order to modify a sub-report, highlight the report name, use the right mouse button and select **Edit Report** from the menu options.

2 The **Report Edit Dialog** will display. The Description and Notes fields can be modified. The Report File Name cannot be changed, however, it is displayed for reference. You will also find the Date Created and Date Last Run fields here.

Deleting a Sub-report

1 Highlight then right-click the report you want to delete and click the **Delete Report** menu option or right click and select Delete Report from the menu. The software will not permit the deletion of Base and Derived reports.

Viewing Report Selections

If there are any selections for a sub-report, such as cardholders, devices, or areas, these selections will be displayed on a tabbed page at the bottom of the report launcher when the Derived Sub-report report is highlighted in the tree. The following page will show the displayed information for a Derived report.

You can include additional selections to any Derived Sub-Report by clicking the **Add Selection** button. To remove selections, highlight the records you want to remove and click the **Delete Selection** button. For each selection type that the report has, another tab will be displayed.

Chapter 11: Manual Overrides

Introduction

Geoffrey **Manual Overrides** Program allows the operator to manually change a device's normal function, possibly to allow temporary access to an area to exit in an emergency situation. There are two modules that comprise the overall function: **Manual Override Definition**, and **Manual Override**. Manual Overrides are programmed, or defined using the Manual Override Defintion module. They consist of sets, tasks and their actions. An Operator must physically execute the Override command whenever necessary. Manual override sets are defined so that several devices can have commands sent to them simultaneously. For instance, if you want to have all perimeter doors unlock in an emergency, you would define manual overrides with the appropriate commands to control the devices for those doors. If an emergency arises, the authorized Operator will select the "emergency" override and execute it.

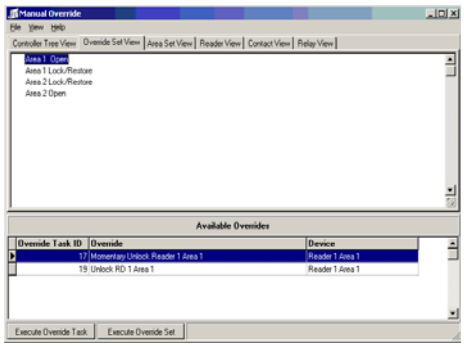
In Manual Override Definitions, all the programming for Override Sets, Tasks and Actions was completed in order for Authorized Operators to execute necessary actions using this module. The range of actions is limited only by the Security permissions granted to the individual or group in System Security.

Accessing the Application

1. Open the Geoffrey Launcher by double clicking the Launcher icon on your desktop.
2. The login window, opens. Enter your user id and password.
3. In the System Launcher window, double click on **Manual Overrides** icon.

Overivew

The top portion of this window contains several View tabs. Selecting these buttons selections from the View menu will bring forward the tab you wish to use to locate or view override records. The bottom portion entitled Available Overrides, displays any defined tasks that exist for the currently highlighted record in the view above.



Executing Manual Overrides

1 **Controller Tree View –** Navigate through physical connections to locate Overrides by device. Select the override and click **Execute Override Task** button located at the bottom of the window. .

2 **Override Set View –** This is the default tab. Highlight a Set or Task to execute it, both buttons are available here. (**Execute Override Task** and **Execute Override Set**)

3 **Area Set View -** Navigate through Areas to select overrides defined for devices in an Area. Override Sets are not available in this tab.

4 **Reader, Contact and Relay Views - The** devices included in the currently defined Overrides are displayed. The Device ID (#), device name and Area information is provided. Individual Tasks may be executed under these tabs.

Note: *The permissions granted to individual operators determine what will be available for display and execution in any of these views. Please refer to the System Security chapter for details.*

Chapter12:Security Tour System-Client

Introduction

The **Geoffrey Security Tour System** is an essential tool for any company that provides guard services. It is designed to provide valuable and timely information to ensure high level of efficiency and safety. This Tour System is a complete solution for tracking and evaluating your security personnel, as well as provide your clients with clear, concise reports, in which you can guarantee that the job was completed.

The Security Tour System is a Windows Client application that will allow definition of tours, real-time tracking of running tour progress, alerts when tour criteria is not satisfied, and historical reporting of previously run tours.

This system has two modules; the **Security Tour Editor** and the Tour Client. Definition of tours, checkpoints, settings for tour status, and checkpoint status are done using the Security Tour Editor application. The tour client application allows the user to monitor the tour status and checkpoint status. This chapter describes the operating instructions for the **Security Tour Client Module**.

Note: *Make sure that SP, CIM and the Tour Service application are running before you start the Tour-Client application.*

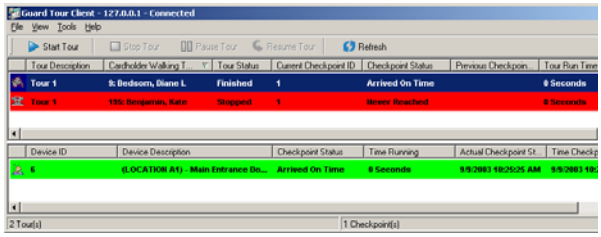
Accessing the Application

1 Open the System Launcher by double clicking on the Geoffrey Launcher icon on your desk top.

2 Select **Security Tour-Client** icon and double click on it.

Overview

The Security Tour System application also allows the user to start new tours, stop, pause and resume currently running tours.



The main window of the application displays the tour status and checkpoint status. The status messages are displayed according to the colors and fonts selected for each message in the Tour Definition Client application. The upper pane of the window displays the tour definition information including tour status, cardholder information, checkpoint status etc. The lower part of the window shows the device details and checkpoint information.

Starting a Tour

1 Select **File>Start Tour** or click on the **Start Tour** button on the tool bar.

Note: *If the first checkpoint defined in the system is an initiator checkpoint, the tour will begin only with a card swipe or a contact transaction.*

2 In the **Start New Tour** window, first select the tour you want to start. Click on the expand button near the **Tour to Start field** to select a record from the defined list of tours.

3 Next, click the expand button to select a cardholder who will walk the tour. In the **Cardholder Search and Select** window, you can run a search by entering the last name or first name of the cardholder in the corresponding fields.

4 Once you select the cardholder, click **Start Tour**. Clicking **Cancel** aborts the process.

Description of Fields

Once a tour has begun the following columns display the information corresponding to each field.

Upper Section

Note: *The columns appear on the upper section of the main window of the application are sortable and not necessarily be in the order that is described below. The changes will be saved.*

1 **Icon** - A picture that shows the current status of the tour.

2 **Tour Description** - The name of the tour that is given in the Tour Editor application.

3 **Cardholder Walking Tour** – The name of security officer who is going to or is currently walking the tour.

4 **Tour Status** - The current status of the tour. E.g. Running, Stopped, Timed Out etc.

5 **Current Checkpoint ID** – The identification number of the current checkpoint.

6 **Checkpoint Status** - A status message is displayed indicating the status of the current checkpoint. E.g. Arrived Early, Arrived Late.

7 **Previous Checkpoint** - The status of the previous checkpoint.

8 **Tour Run Time** - The amount time the tour has been running. If the first checkpoint is an initiator checkpoint then this time will not start until that checkpoint has been reached.

9 **Time Tour Created** - This field shows the time the tour was created by the operator.

The following menu options are displayed when you right click the tour grid.

10 **Remove Tour** (also Delete key and Main Menu\View\Remove Selected Tour) - This button will only display if the currently selected tour is stopped or finished. When used, the selected tour will be deleted from the list.

11 **Remove All Finished and Stopped Tours** (also Shift-Control keys and Main Menu\View\Remove All Finished and Stopped Tours) - Choosing this option will remove all the finished and stopped tours from the list.

Lower Section

Note: *The columns under this section cannot be sorted. Checkpoint always display in the order they are supposed to be reached.*

1 **Icon** - A picture describing the current status of the checkpoint.

2 **Device ID** - The identification number of the device that is acting as the checkpoint.

3 **Checkpoint Status** - The status of the checkpoint. E.g. Arrived Early, Arrived Late.

4 **Time Running** - The amount of time the checkpoint has been waiting to be reached.

5 **Actual Checkpoint Start Time** - The time that the cardholder supposed to reach the checkpoint.

6 **Time Checkpoint Reached** - The time the checkpoint was reached.

7 **Time Allowed to Arrive** – The amount of time the cardholder walking the tour can take to reach the checkpoint. This will start when the previous check-point was reached.

8 **Checkpoint ID** – The identification number of the checkpoint.

View Cardholder Image

1 To verify the image and/or signature of the security officer who is walking the tour, select the tour and choose **View>Cardholder Images** option from the menu.

Stop, Pause, Resume Tours

1 To stop a tour, select the tour and click on the **Stop Tour** button on the tool bar or select **File>Stop Selected Tour**. This option will only become enabled when the selected tour is running or paused

2 To stop a tour for limited amount of time select Pause Tour button or **File>Pause Selected Tour** option from the menu. The Resume Tour button must be used to re-start the tour. If the tour is paused for longer than the idle time-out period of the tour, the tour will automatically be cancelled. The Pause Tour button will only become enabled when the selected tour is running.

3 To re-start a stopped or pauses tour click the REsume tour button or **File>Resume Selected Tour** option from the menu. The resume tour button will only become enabled when the selected tour is paused.

Removing Tours

1 To delete a tour from the view select the tour and choose **View>Remove Selected Tour** option.

2 To delete all stopped or finished tours select **View>Remove All Finished or Stopped Tours**.

Index

A

Access Control Badge 2
Access Control Cards 3
Access Denied Transactions 57
Acknowledged and Not Secured 31
Acknowledging Alarms 31
Acronyms 1
Active Alarms 31
Active Badge Options 10
Active Badge Options 10
Add Badges 10
Add New Cardholders 6
Add New Cardholders 6
Adding E-mail Addresses 22
Adding E-mail Addresses 22
Advanced Find Feature 26
Alarm Acknowledgement 41
Alarm Acknowledgement 41
Alarm Graphics Client 41
Alarm Information 30
Alarm Maintenance 35
Alarm Monitor 30
Alarm Notification 41
Alarm Notification 41
Alarm Types 38
Archive History 53
Area Access 8
Assigning Areas, Area Sets 7
Assigning Areas, Area Sets 7
Assigning Areas, Area Sets 7
Audit Trail Report 59
Auto-load the Saved Monitor 49

B

Badge Definition
Badge Definitions
Base Reports 64

C

CIM and SP Status Messages 54
CIM to RC Communications 54
Card Alarms 38
Cardholder Definition 5
Cardholder Definitions
Cardholder Search Wizard 26
Client application 69
Communication Interface Module
Communications Alarms 38
Contact Alarms 38
Controller Alarms 39
Creating a new report 65
Credential Insert Full Automation Mode 12
Customer Support 3
Customize the Transaction Code 48
Customize the Transaction Code 48
Customizing the Transaction Monitor 48
Customizing the Transaction Monitor 48

D

Default State of an Icon 45
Define Offline Lock Access 20
Defining a Monitor 48
Delete Cardholders 24
Delete a Single Cardholder record 24
Deleting E-mail Addresses 23
Deleting E-mail Addresses 23
Deleting a Sub-report 66
Derived Sub Report 64
Device Control 55
Download/Update Status Messages 55
Duplicate Cardholder Information 22
Duplicate Cardholder Information 22

E

Editing Transaction Monitors 50
Editing Transaction Monitors 50
Edting Offline Credentials 16
Executing Manual Overrides 68
Executing Override Tasks 35
Export Cardholder Portraits 24
Exporting Data 16
Extend Area Access Time 8

F

File Server
Film separations
Filtering Transactions 49

G

Generating Badges Automatically 11
Generating Badges Automatically 11
Guest Alarms 39
Guest Pass Transaction 55
Hours of Support 3

K

Key Features 2

L

Labels 2
Launching a Report 64
Launching the Portrait Monitor 57

M

Manual Overrides 67
Manual Overrides within Portrait Monitor 58
Massive Access Control Modification for Cardholders 23
Minimize Alarm Monitor 35
Modify Area Access 8
Multiple Cardholder Deletions 24

N

New Cardholder Wizard 6

O

Offline Credentials 13
Operator Alarms 39
Overview 47
Overview 5

P

Page creep. See Creep
Pausing Transactions 48
Popup on Transaction 49
Portrait Capture 9
Portrait Capture 9
Portrait Monitor 56
Pre-defined Alarm Comments 32
Pre-defined Alarm Comments 43
Print Alarm Screen 35
Printing
Printing Reports 25
Printing and Exporting Reports 64

Q

Quick Launch Feature 64

R

Reader Controller 3
Reader Interface 3
Rearranging and sorting Column Titles 62
Receiving Video of Alarms 33
Refresh Report 61
Registration. See Misregistration
Relay Alarms 38
Relay Alarms 38
Relay Transactions 55
Removing Tours 71
Report Launcher 63
Report Tree View 63
Retire Badges 13
Retire Credentials 21
Reviewing proofs. See Proofing
Run Report 61
Running a Report 36
Running a Report 36

S

Screen frequency. See screen ruling
Search for Icons and Maps 45
Security Tour Client Module 69
Security Tour System 69
Security Tour System Transactions 55
See also Separations
Select a Category 9
Signature Capture 9
Starting a Tour 70
Starting the Alarm Monitor 30
Stop, Pause, Resume Tours 71
System Alarms 39
System Components 2, 3
System Overview 1
System Processor
System Software

T

Tour System Alarms 40
Transaction monitor 47

U

Understanding a Report 61
Use of Wildcards 27

V

View Alarm Comments 37
View Cardholder Image 44
View Cardholder Image 44
View Previous Alarms 36
View Previous Transaction 52
Viewing Previous Alarms 35
Viewing and Editing Cardholder Information 34

W

Working with the Portrait Monitor 57
Working with the Transaction Monitor 48
Working with the Transaction Monitor
Workstations